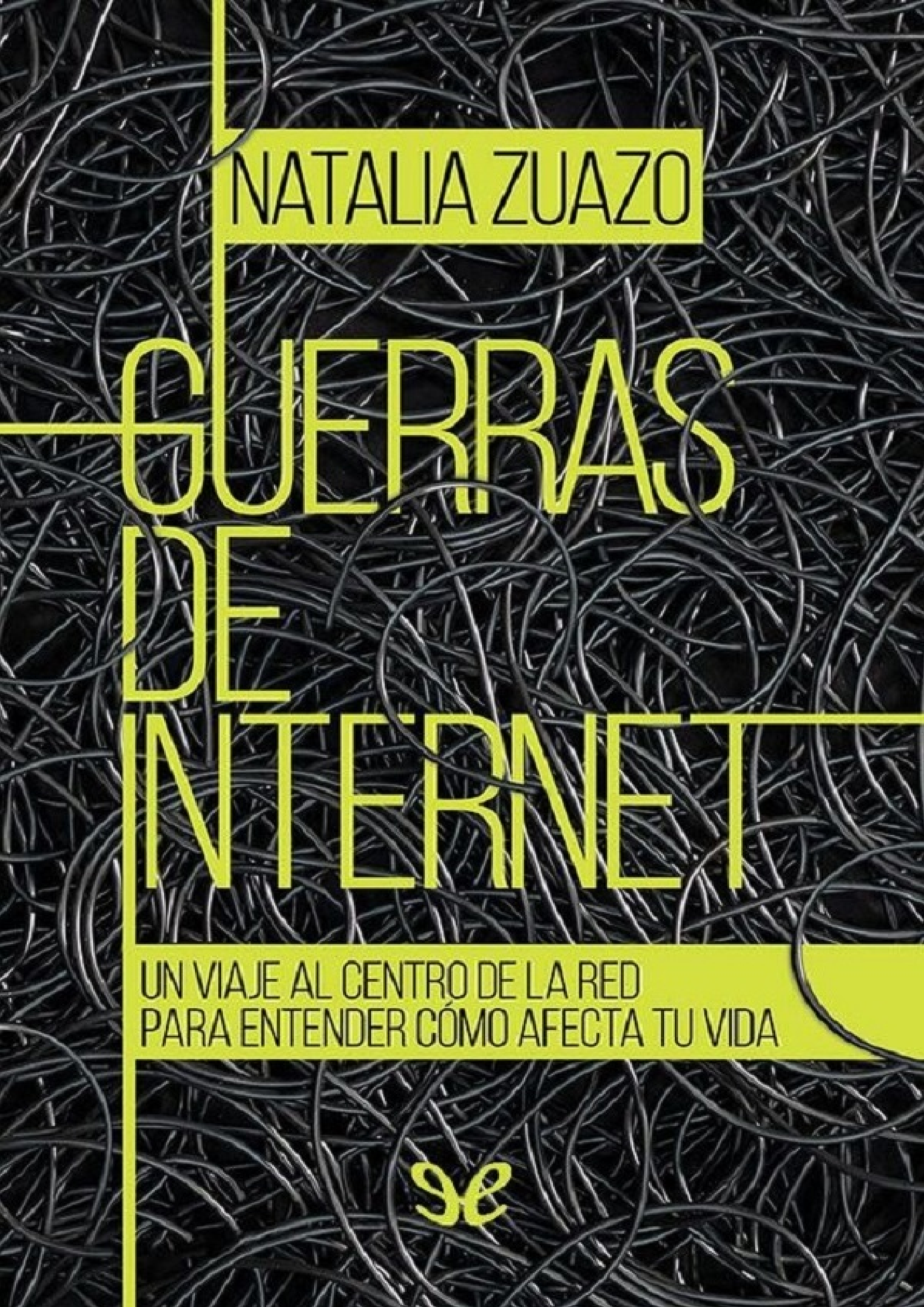

NATALIA ZUAZO
GUERRAS DE INTERNET
UN VIAJE AL CENTRO DE LA RED
PARA ENTENDER CÓMO AFECTA TU VIDA

Internet está tan presente que prácticamente no pensamos en ella. Ya ni siquiera nos exige conectarnos a un cable: se desmaterializa y desaparece entre las paredes y los muebles de nuestra casa, nos rodea con ese halo mágico llamado *wifi*, que no vemos pero nos mantiene comunicados mientras chequeamos un *email* en la terraza o nos acostamos a la noche a ver una película.

Con su omnipresencia que todo lo resuelve, internet se erige como la primera religión común de la humanidad y nos aterra la idea de estar desconectados por más de un segundo. Pero confiar tanto en cualquier poder tiene sus riesgos.

En este libro, Natalia Zuazo se propone bajar la tecnología del pedestal y contar las historias humanas más allá de Internet para nombrar a los protagonistas, saber cómo funciona, entender cuáles son las luchas de poder que hay detrás, qué hacen las empresas y los gobiernos con nuestros datos, y cuánto de todo esto sabemos o ignoramos.



Natalia Zuazo

Guerras de Internet

ePub r1.1
Titivillus 09.04.2020

Título original: *Guerras de Internet*
Natalia Zuazo, 2015
Diseño de cubierta: César Pucciarello

Editor digital: Titivillus
ePub base r2.1





A los cambios. Y a los valientes.

«Hay algo casi sagrado en internet.
Yo estoy tratando de secularizarlo».

EVGENY MOROZOV.

«La manera como se presentan las cosas no es la manera como son; y si las cosas fueran como se presentan la ciencia entera sobraría».

KARL MARX.

«La historia de las luchas de poder, y en consecuencia las condiciones reales de su ejercicio y de su sostenimiento, sigue estando casi totalmente oculta. El saber no entra en ello: eso no debe saberse».

MICHEL FOUCAULT.

Prefacio

Internet en el pedestal

> «Es necesaria una mirada menos ingenua sobre las máquinas y los procesos técnicos, una mirada no ajena a la curiosidad pero también escéptica y alerta. ¿Qué ocultan, qué sostienen los aparatos?».
>
> CHRISTIAN FERRER.
> *El entramado* (2012).

> «Entendemos cómo funciona el poder en el mundo físico, pero todavía no entendemos bien cómo funciona el poder en el terreno digital. Internet es una creación humana. Las luchas de poder son una parte inevitable de la sociedad».
>
> REBECCA MACKINNON.
> *Consent of the Networked* (2012).

Cuando empecé este libro decidí escribir «internet» con minúscula. Casi todos, todavía, lo hacen con mayúscula otorgándole una importancia de cosa única, un nombre propio.

Ya pasaron más de veinticinco años desde que usamos internet tal como ahora lo hacemos: un conjunto de redes conectadas con otras a lo largo del mundo que nos permiten intercambiar información con otros. Desde esa función de medio de comunicación tan cotidiana —como la telegrafía primero, los teléfonos o la radio después—, internet tendría que sumarse a esos inventos que se fueron acumulando para reducir distancias y hacernos la vida más cómoda.

Internet está tan presente que ya no la pensamos. Ya ni siquiera nos exige conectarnos a un cable. Como la electricidad, otra creación humana que suponemos siempre dispuesta a hacer funcionar las cosas, está siempre allí para darnos la energía artificial que mueve todo. Internet está tomando el mismo camino: se está volviendo omnipresente e invisible. Se desmaterializa y desaparece entre las paredes y los muebles de la casa, nos rodea en ese halo mágico llamado *wifi* que no vemos pero nos mantiene conectados mientras colgamos la ropa y chequeamos un *mail* en la terraza o cuando nos acostamos para ver una película que alguien subió a YouTube. Con los dispositivos móviles también seguimos *online* fuera de casa, cuando subimos al auto,

en el viaje en el subte, o en los aparatos que llevamos con nosotros cuando salimos a correr y comparten la distancia y las pulsaciones que medimos a nuestros amigos en las redes sociales. Siempre conectados, ya no pensamos en «subir» o «bajar» el interruptor. Nos aterra la idea de estar desconectados más de un minuto. Entramos en pánico si «se cae» la conexión: cuando eso ocurre, nosotros también nos caemos del mundo.

Internet, con su omnipresencia que todo lo resuelve, se erige como la primera religión común de la humanidad. Confiamos tanto en su poder que le damos un lugar en el cielo, donde también imaginamos a Dios, cualquiera sea su forma para nosotros. No es casual que la publicidad, la gran difusora de toda novedad en el mundo, también haya construido la imagen de internet en el cielo como una «nube» que se posa sobre todos nosotros para mantenernos conectados. Esa representación blanca, luminosa, etérea, sin cables ni fallas, se presenta como el espacio donde todos los problemas tienen solución, donde estar conectados es ser felices. Una internet así de poderosa merece ser escrita con mayúscula.

Yo, en cambio, me opongo a esa idea.

Confiar tanto en cualquier poder del mundo nos impide cuestionarlo y nos vuelve demasiado sumisos a sus encantos. Tratar a internet como una religión universal tiene muchos riesgos. Este libro se propone enfrentar esos riesgos y contar las historias humanas de internet para hacerla *real*, para darle nombres a sus protagonistas, para saber cuáles son los caños que atraviesa para funcionar, quiénes la controlan, quiénes quieren hacerla invisible y cuánto de eso sabemos o ignoramos. Este libro se introduce —concretamente— adentro de la Red[1] para acercarla a nuestra vida cotidiana, aquí y ahora, en la Argentina. Para eso, baja la tecnología del pedestal blanco y prolijo de la publicidad y se pregunta cómo funciona, cómo llega a nuestra casa, a quién se la compramos y cuánto dinero ganan sus empresas cada vez que la usamos. Y trata a internet con minúscula para explicar cosas que se suelen ocultar: quiénes son sus dueños, quiénes hacen sus leyes (las que vemos y las que no), por dónde circulan nuestros datos y qué hacen con ellos las corporaciones y los gobiernos. La trata con minúscula para materializarla. Porque cuando dejamos de pensarla como si fuera un dios aparecen otras fuerzas, menos prolijas y equilibradas: las del poder, que luchan por imponerse, que hacen guerras, que se deciden en las mentes y los escritorios de mujeres y hombres.

En el caso de internet, por cierto, hay más hombres que mujeres. En el recorrido de este libro, me encontré con un mundo casi despoblado de lo femenino. También descubrí que es un universo pequeño donde todos se conocen, como en un barrio, aunque sean millones de hombres los que componen las piezas del monstruo de internet del mundo. La primera reacción de estos hombres que me recibieron para responder mis preguntas (ingenieros, funcionarios, gerentes, técnicos de redes) fue la sorpresa ante la irrupción de una mujer curiosa en ese universo tradicionalmente masculino. Sin embargo, al rato de hablar y cuando les planteaba algunas preguntas

que nadie les había hecho, reaccionaban como niños que ven llegar a su madre después de un día de trabajo: querían contarme mucho más de lo que mi mano era capaz de anotar, me abrían sus mundos secretos de cables, se quedaban durante horas explicándome cosas que solo hablaban con otros ingenieros o funcionarios, pero nadie «de afuera» les había pedido contar nunca.

Hay mucho que contar de internet todavía. Y es el momento de contar internet de otra manera.

El sociólogo Christian Ferrer dice que, en la década de 1990, el ideal de internet era el modelo «Benetton», una especie de sociedad global donde todos los habitantes del mundo se entienden entre sí. Ese ideal todavía persiste cuando nos paramos en la tierra y miramos hacia el cielo buscando las respuestas en la tecnología, pensando que nos va a resolver todos los problemas, desde ahorrarnos tiempo de trabajo hasta encontrar sexo (¿y amor?) a un clic de distancia. Pero en los últimos años comenzamos también a ver las primeras contradicciones y luchas. Gracias a los activistas por las libertades de internet, a grupos de *hackers*, a organizaciones como WikiLeaks que filtraron cables diplomáticos de gobiernos, a la valentía de exconsultores de organismos de inteligencia como Edward Snowden que reveló que Estados Unidos espiaba a todos sus ciudadanos, o a *hackers* develando secretos alrededor del mundo, empezamos a enterarnos que internet no sirve solo para hacernos la vida más fácil. Hoy también sabemos que las empresas la usan para recabar datos personales y vendernos cosas, que los gobiernos desarrollan herramientas para espiar a ciudadanos y a otros poderes, que ninguna aplicación gratuita realmente *es* gratis del todo y que la tecnología también puede servir para impulsar guerras.

Nací unos días antes de 1980 en Tolosa, un antiguo barrio ferroviario de La Plata, capital de la provincia de Buenos Aires, Argentina, famosa por sus universidades y su trazado urbano modelo. Dos años antes, la televisión a color había llegado al país. En mi casa había libros, revistas y sobre todo varias enciclopedias —mis favoritas—, con las que pasaba mucho tiempo, leyendo y revisando el funcionamiento de todas las cosas, y especialmente mirando mapas: países, océanos, ciudades, capitales, los planetas y el universo. Me quedaba perpleja frente a los recorridos de caminos, rutas y construcciones. Después, la curiosidad se desplazaba de la teoría a la práctica, a cómo funcionaba ese mundo desde adentro. Pegaba varias hojas haciendo una línea recta y dibujaba los detalles de los inventos humanos a lo largo, como en los mapas de la escuela, donde todo se traduce a un plano. Era mi forma de entender.

En 1987, cuando pocas familias tenían computadora, mi mamá ganó el quinto premio del Gordo de Año Nuevo de la Lotería y compró una IBM PS/2. Era pesada, de un plástico duro color crema, con teclas altas y duras. Le compramos una mesa grande y resistente, como un altar. La usamos por un tiempo como máquina de

escribir familiar y yo la usaba para practicar algunos ejercicios simples de programación que aprendía a la mañana en una escuela de inglés bastante adelantada a su tiempo. En los 80, las computadoras eran el futuro. La publicidad —el negocio inventado para convencernos de adoptar lo nuevo porque siempre es mejor que lo anterior— las mostraba como elementos de paisajes de ciencia ficción, pero también como objetos imprescindibles de la evolución humana. En 1984, un comercial de Commodore 64, una de las primeras computadoras familiares populares, mostraba a todas las generaciones, desde los abuelos hasta un bebé, en un primer plano iluminado y preguntaba: «¿Cuán viejo serás?», con clara voluntad de «no te quedes atrás de este cambio». El mismo año, Ridley Scott dirigía un famoso aviso para Apple, inspirado en la novela apocalíptica de George Orwell, justamente *1984*, pero para resignificarla: las computadoras, en manos de una atleta que corría con un martillo olímpico entre cientos de hombres grises uniformados, venían a romper con la opresión para hacernos libres en un nuevo mundo de conocimientos.

Sin embargo, en los 90, la libertad pasó a un ámbito menos utópico. La publicidad de la tecnología tenía que ver con el trabajo y la eficiencia. En la década del crecimiento del mundo financiero globalizado y la concentración económica, poseer lo más nuevo era ser más productivo. Y ser más productivo era ganar más dinero, el alimento básico del *yuppie*. Pero ese superhombre de traje y hombreras tan bien representado en la novela y película *American Psycho* ya no estaba tan aislado. En 1989, el científico inglés Tim Berners-Lee creó el lenguaje HTML y su equipo de trabajo le dio forma al primer servidor web. Fue exactamente el 12 de marzo de 1989. Nacía la *World Wide Web*, las conexiones salían del uso militar o universitario y llegaban a otras personas, a partir de allí llamadas «usuarios». Internet comenzaba a expandirse masivamente y la tecnología vivía su gran momento de optimismo. Adoptarla era progresar, conectarse era quedarse del lado de adentro del planeta. En ese mundo, la publicidad le daba forma a un nuevo héroe, el nerd, que se transformaría en un *rockstar* con un talento que sería cada vez más valorado: leer y escribir códigos o programas, es decir, comprender el lenguaje de las computadoras, que también era el idioma del nuevo mundo.

En Argentina, internet empezó a llegar masivamente a los hogares entre 1993 y 1995. Mi primera conexión fue en 1994, y fue también la de toda mi familia, reunida frente a la computadora (todavía eran un objeto compartido entre los integrantes de la casa y no un elemento personal e intransferible, como hoy). Un viernes a la tarde, cuando ya habíamos vuelto de la escuela y el trabajo, nos reunimos frente al monitor y mi novio adolescente experto en redes hizo una conexión desde el gabinete de la computadora hasta el teléfono. Escuchamos el ruido de la conexión durante quince segundos mientras en la pantalla se dibujaba una línea roja que conectaba un receptor con un *router*. Ya conectados, empezaron las peleas. Todos queríamos entrar en una página distinta, en un jueguito, a abrir una cuenta de *mail*. Los jóvenes de la familia nos impusimos. Dominamos por un rato el módem. Pero conectarse todavía era muy

caro y las aventuras virtuales duraban lo que nuestros padres soportaban, distraídos con otra cosa.

Internet crecía. Las empresas de telecomunicaciones instalaban cables y tubos que cruzaban el mar y la tierra. Se colocaban kilómetros nuevos de fibra óptica y se construían servidores para almacenar cada vez más datos. Fue una expansión sin plan maestro: la infraestructura de internet aumentó a medida que empresas, gobiernos, universidades y usuarios quisieron y necesitaron usarla. Por supuesto, también creció porque fue el nuevo gran negocio de las empresas de telecomunicaciones. La publicidad y los augurios de los gobiernos, que abrazaron «la sociedad de la información» como una forma de «estar dentro del mundo», también se encargaron de hacerla crecer en la imaginación.

Mientras esta expansión horizontal sucedía, Estados Unidos estableció una serie de instituciones que iban organizando verticalmente —y apropiándose— de las funciones técnicas de la Red: la distribución de las direcciones, los nombres de dominio, los servidores donde se almacenan los datos. El mundo se llenó de cables y edificios que generalmente no vemos porque no tienen grandes carteles, pero nos rodean y son el sustento material de internet, una parte fundamental de su lógica y funcionamiento, pero que muchas veces ignoramos. Y no por casualidad.

Desde el año 2000, que daba inicio a la década que la ciencia ficción asociaba con el futuro, el *marketing* de la tecnología dejó de vender objetos, eficiencia y productividad. Empezó a vender otra cosa: estar conectado era vivir emociones. Y que ese mundo de felicidad estaba lejos, en una nube.

Según la retórica y el derroche visual de la publicidad, internet es una estela invisible que recorre cielos celestes donde los datos (mensajes, *mails*, fotos, gatitos que juegan en YouTube) se cruzan y llegan a la computadora o el celular de gente joven y linda —o vieja y saludable— que se abraza a la distancia o baila con sus auriculares en una plaza.

Pero la internet real es bastante distinta de esa imagen. Internet es ese mundo lleno de tubos, cables, tierra, agua, arena y centros de datos aburridos con luces que se quedan solas de noche titilando sin fiestas ni plazas soleadas alrededor.

Cuando empecé este libro también hice una encuesta. Le pedí a cincuenta personas, de diversas edades y profesiones, que me dijeran qué era para ellos internet, cómo funcionaba y quiénes la manejaban, por dónde pasaban sus datos. Les pedí, también, que me dibujaran internet. Con las respuestas en la mano, comprobé que la idea de internet como una nube que nos sobrevuela está muy instalada en nuestra imaginación acerca de qué y cómo es la Red. En cambio, muy pocos trazaron cables en el fondo del mar o asociaron internet a la tierra. La mayoría respondió «no sé» ante la pregunta de si existen leyes que regulen lo que hacemos en internet y una gran parte dio la misma respuesta sobre el camino y el destino de los datos que suben o bajan de la Red. La encuesta, aunque no fuera científica, me hizo confirmar mi plan: tenía que salir a *contar* internet.

¿Pero cómo *contar* internet? ¿Cómo hablar de algo que todavía pocos dominan pero de lo que todos hablan, con optimismo (consumista, civilizador, emancipador) o pesimismo («nos aísla», «nos invade», «nos espía»)? Propongo contar internet recorriendo ese camino que queda entre las dos emociones extremas que despiertan las tecnologías: la del miedo y la de la libertad.

No soy técnica; este no es un libro técnico. Estudié Ciencia Política y trabajo como periodista hace quince años. Escribo sobre tecnología, pero antes de empezar esta investigación sabía más o menos lo mismo que un curioso de las computadoras o las transmisiones de internet. Sé cosas muy básicas de programación y me enfrento al mismo estrés que cualquiera cuando mi proveedor me deja sin conexión. Sin embargo, como periodista que hizo su carrera en una redacción digital y como estudiosa del poder, fui juntando algunas preguntas sobre internet. Casi siempre, lo que no se responde es porque no conviene. Conocerle la cara a los dueños de la tecnología, saber que el mundo perfecto de la nube es un poco más gris o que quienes dicen guardar nuestros datos no lo hacen siempre para cuidarnos implicaría vender menos aparatos y conexiones.

Sin embargo, lo desconocido sobre la tecnología no siempre es producto de una conspiración o la maldad humana. Yo misma soy parte de la «industria» de internet: trabajo en medios digitales y hago que la gente use internet para leer, buscar y consumir cosas. Soy optimista y difusora de muchas de sus herramientas, sobre todo las colaborativas, las que permiten hacer sitios como Wikipedia o compartir las distintas formas del arte a través de un archivo de *torrent*. Pero también, como periodista que se dedica a la tecnología, me enfrento a que, en la mayoría de los casos, las miradas de mis colegas son ingenuas, centradas solamente en presentar «lo nuevo», corriendo siempre para mostrar el aparato que reemplaza al anterior, de la novedad como garantía de felicidad. Algunos comunicadores vivimos una suerte de exclusión cuando decimos que la tecnología es más compleja. ¿Conflictos, miedos, monopolios informativos, decapitaciones en YouTube, pedofilia, vidas que ya no son privadas, empresas que saben todo de nosotros? «No, eso no es para la tecnología», parecen decirnos. «No: la tecnología siempre es avance, siempre es más debate, más democracia», dicen otros.

Pero yo sí tengo algunos miedos. Me preocupa especialmente el desarrollo de las tecnologías (de países o de empresas) orientadas a controlar las vidas de la gente, con la excusa de hacerla más fácil o de proteger la seguridad. Me inquieta que la conexión crezca más en ciertas zonas del mundo, como todo producto del capitalismo. No porque la llegada de internet vaya automáticamente a civilizar a los no conectados. Sino porque es otra forma de desigualdad. Me preocupa que no podamos ver algo que la escritora y activista norteamericana Rebecca MacKinnon explica con elocuencia: le damos un poder excesivo a internet porque el valor supremo es estar conectados, pero no nos preguntamos quién la controla ni qué hace con nuestra información. El problema es que la libertad de todos depende cada vez

más de quién controla esa información que está en internet, pero que la manejamos nosotros, los humanos. Los seres humanos escriben las máquinas y los programas que la manejan. Los seres humanos siguen haciendo las leyes. Y las leyes, en el caso de internet, están en los códigos[2].

Sin embargo, cualquiera de estos miedos se resuelven, primero, con un gran antídoto: la información. Y para buscar esa información escribí este libro, que se basó en algunas preguntas:

¿De quién son y por dónde pasan los caños que nos conectan?

¿Quién hace las leyes de internet? ¿Quiénes son esos hombres y mujeres y a quién responden?

¿Cuál es el camino de los datos que subimos a la Red? ¿Quién y cómo los maneja?

¿Cómo se usa la tecnología para controlarnos?

¿Quién escribe los códigos que manejan nuestras vidas?

Probablemente, algunas de estas respuestas estén en Google. Pero Google, aunque me parece un invento fascinante y sumamente útil, también es una máquina creada por seres humanos que inventaron un algoritmo[3] que ordena las respuestas de una manera, dando prioridad a algunas y dejando más abajo otras.

En cambio, las respuestas de este libro las van a dar las personas que fui conociendo en el camino, a partir de mis preguntas y mi internet vista con minúscula, para que entrara en una máquina de rayos X de tubos, de mapas, de leyes, de servidores que almacenan datos, de hombres que manejan esa información con distintos fines. Para verla en una escala más real. Para saber cómo está escrita. Y para algún día escribir otros algoritmos. O no, pero al menos para saber cómo funcionan los que usamos.

Irrumpir de cerca en la tecnología para deshacerla y contarla es la primera forma de acercarse a los conflictos de hoy y del futuro. Los fierros, las redes y los aparatos que nos hacen la vida más fácil están hechos por personas y corporaciones. Los usan los gobiernos, las empresas, nosotros. Para cada uno son distintos, pero nunca neutrales. Las máquinas también hacen política.

El viaje comienza en el fondo del mar. La primera parada es un lugar pequeño y poco conocido de la Argentina, donde un grupo de hombres cuida y conecta una de las partes fundamentales del monstruo de internet. Allí, en los caños, empiezan las guerras.

PRIMERA PARTE

De la nube al fondo del mar: Cómo funciona internet (realmente).

I

Las Toninas: mate, playa y cables submarinos

> «La Naturaleza está imitada de tal modo por el arte del hombre, que este puede crear un animal artificial».
>
> THOMAS HOBBES.
> *Leviatán, o La materia, forma y poder de una república eclesiástica y civil* (1651).

—Nos van a poner una bomba.

El comerciante se animó a decir lo que todos comentaban por lo bajo. Fue el primer valiente de la reunión que hasta ese momento se desarrollaba en la paz de un invierno húmedo de 1999. Pero la tensión se acumulaba.

Las Toninas, un balneario modesto de cinco mil habitantes a trescientos kilómetros de la ciudad de Buenos Aires, sufría una invasión sin precedentes. En sus calles de tierra, se desplegaban grúas, obradores y mezcladoras de cemento. En el puerto se estacionaban barcos de más de cien metros de largo que encendían sus luces a la noche y se iluminaban como si fueran una ciudad flotante. La pizzería del pueblo, acostumbrada a recibir empleados públicos y comerciantes al final del día, comenzó a recibir a belgas que bajaban de los barcos pidiendo cerveza, una tras otra, desde la mañana. Durante meses, los vecinos de Las Toninas no supieron ni entendieron nada. Encargaron más botellas de cerveza y mejoraron el plato del día para el almuerzo, pero nadie les daba más pistas. Mientras tanto, la costanera ancha se colmaba de montículos de arena y cerca de la ruta se levantaban dos nuevos edificios, bajos y grandes como supermercados.

Lo que los vecinos ignoraban era que ese misterio los haría famosos. Ignoraban también que por el mar y la arena estaban entrando los cables submarinos de internet que conectarían a la Argentina con el mundo. No podían ver que dentro de los nuevos edificios se estaban instalando filas largas de estantes con servidores y conexiones de fibra óptica. No sabían que esta pequeña ciudad de 5200 habitantes se estaba transformando en lo que la haría para siempre conocida. Las Toninas se estaba convirtiendo en «la capital nacional de internet».

Los habitantes navegaban en rumores: se decía que estaban instalando ese nuevo monstruo de las comunicaciones llamado internet. Pero que no se trataba de simples conexiones sino de su columna vertebral, unos tubos larguísimos que salían de los flamantes edificios y se metían al mar. Era auspicioso ser el centro de algo, pero

también les daba miedo. ¿Y si alguien quisiera romper los cables? ¿Quién los protegería si pusieran una bomba para hacer volar el futuro por los aires?

Ante el pánico, las empresas de telecomunicaciones, las mismas que habían quebrado la paz del pequeño balneario, fueron quienes convocaron a la reunión. El Consejo de Ingenieros de la ciudad vecina de Santa Teresita les propuso a las empresas dueñas de los cables —Level 3[4], Telefónica y Telecom— reunirse con los habitantes y explicar qué estaba ocurriendo. Eligieron el salón de usos múltiples de la Sociedad de Fomento de Santa Teresita, el más grande de la zona, y ordenaron en filas las sillas de plástico negro. El primero en llegar fue el intendente. De sobretodo y guantes negros, saludó a los ingenieros del lugar y a los representantes de las empresas y tomó asiento rápido. Él también quería saber más.

El ingeniero Ernesto Curci, que estaba a cargo de la estación de amarre de cables submarinos de Level 3, fue el encargado de dar la primera charla. Su misión era explicar que no había nada que temer. Curci, que tenía cuarenta y cuatro años y acababa de ingresar a la compañía, habló más de una hora. De un metro sesenta de alto, erguido y atlético a base de gimnasio y maratones, ya había participado en la instalación de la primera estación de cables submarinos de Las Toninas en 1994, trabajando para Telefónica. Pero eso había pasado más desapercibido.

Curci siempre resulta el elegido para hablar. Puede describir cosas aburridas para otros, pero que él explica con calma y las hace más comunes, palpables. Parece que nunca quiere romper la paz de su cara, aunque cada tanto se le quiebra cuando sonríe, sin dejar de hablar. Acostumbrado a rodearse de ingenieros, mediciones de transmisiones y electricidad, ese día se enfrentaba a un público distinto, extraño a los desafíos técnicos, pero voraz de información.

Un vecino lo interrumpió:

—Ingeniero, con todo respeto, está muy bien lo de internet. Pero acá tenemos miedo de que le pongan una bomba al cable para cometer un acto terrorista.

Curci caminó por detrás de una mesa que enfrentaba al público y apoyó las manos. Miró al frente y respondió con mucha más sinceridad de la que los invitados esperaban.

—Mire: Si hay alguien con capacidad para poner una bomba en los cables son las mismas empresas de tecnología que los instalaron. Pero no creo que quieran romper sus propias instalaciones —explicó Curci, en medio de un murmullo y algunas risas furtivas de los estudiantes de Sistemas de la Universidad Atlántida Argentina de Mar de Ajó, que también habían sido invitados—. En todo caso, si quieren hacer volar los cables, es más fácil hacerlo en cualquier lugar del mar, donde no hay tantos sistemas de seguridad. Y si es por terrorismo, sería más efectivo bombardear una destilería de petróleo y cortar el suministro eléctrico de la zona. Sin electricidad, los cables no podrían transmitir internet.

Quince años después, cuando recuerda la anécdota, Curci sonríe con cariño. Reconoce que el miedo a la bomba en 1999 resultaba comprensible. Internet recién

estaba naciendo y sus promotores la anunciaban con euforia, con la misma parafernalia discursiva con la que habían promocionado la carrera espacial en los sesenta. Era el próximo paso hacia el futuro. Y el futuro siempre crea nuevos miedos.

Curci todavía no sabe si su respuesta dejó tranquilos a los vecinos de Las Toninas. Lo cierto es que, desde que se instalaron los primeros cables submarinos de internet hasta hoy, se conoce en el mundo un solo intento de atentado «contra cables de internet», en Egipto en 2013, y nunca fue del todo aclarado.

Internet no se detiene. El animal puede herirse, pero nunca de muerte. Es tan esencial para los dos mil millones de personas que la usamos a diario como para los infinitos procesos de comunicación de empresas, organismos gubernamentales, fábricas, transportes. La vida moderna funciona y se alimenta de datos. El 95 % de la información del planeta se encuentra digitalizada y está disponible en internet y otras redes informáticas.

Transportar diariamente todos estos caudales de datos es el trabajo de una industria monumental y millonaria. Para eso les pagan a los ingenieros que trabajan en ella («una gran familia», según Curci): para que el tráfico de ceros y unos encuentre siempre rutas despejadas por donde transitar. Para que esto suceda hay que manejar una estructura inmensa, una que emerge desde el mar.

Internet es un gran monstruo en el que todas sus partes están conectadas y se necesitan mutuamente. De eso se trata: redes que se comunican con otras redes, de a millones, en todo el mundo. Sistemas que conversan con otros sistemas. Y lo hacen a través de un idioma en común, una *lingua franca*, el protocolo TCP/IP, una serie de comandos que le dicen a los datos que van viajando que busquen el camino más barato para llegar a destino. Si un camino no está disponible, los datos buscan otro. Prueban una y otra vez nuevas rutas hasta alcanzar su destino. Mientras todo eso sucede, nosotros no nos damos cuenta. Simplemente, esperamos que un *mail* aparezca de la nada en la pantalla o que un video cargue. Son segundos: un sorbo de café, un suspiro frente al teclado, un mensaje que llegó al celular. Pero durante ese instante, el animal trabaja para nosotros. Nunca duerme. Nunca deja de hacer conexiones. Cada parte de su —para nosotros— invisible cuerpo aporta a su movimiento y ninguna puede quedarse quieta. Por eso necesita siempre cargar energía a través de sus cables, ubicados en estaciones de amarre y transmisión como la estación de Las Toninas o en centros de datos (*datacenters*) ubicados en miles de ciudades. Internet es cooperación pura, desplegada en una enorme estructura asentada en edificios en la tierra, pero también conformada por tubos recorriendo todos los kilómetros necesarios para conectar el mundo.

La base de todo ese trabajo, de esas millones de conexiones diarias que nos unen, es física. Son tubos y cables —submarinos y terrestres— instalados por corporaciones o por países que dan la infraestructura necesaria para que esos contactos sucedan, para que los datos viajen, vuelen por las arterias y venas de la bestia. Son redes que corren debajo de nosotros, en la calle por la que caminamos

todos los días, al costado de nuestro escritorio. Son tubos anchos debajo de la vereda o de una ruta, caños más pequeños que llevan cables a nuestra manzana y otros más conocidos por todos (negros, del diámetro de un dedo meñique) que hacen que otro cable se ensamble en el *router* que tenemos al lado y la señal aparezca.

Estamos rodeados por un tejido que no vemos pero sin el cual no podríamos vivir. El esqueleto de internet está allí y un ejército de ingenieros, operarios y marineros lo viene ensamblando desde hace 25 años.

El Leviatán de internet es tan grande como débil. A veces ejerce sus funciones vitales con normalidad: se carga de energía, de luz, hace una sinapsis, manda un dato más lejos y otro más cerca. Durante esos días, los miembros de la legión de guardianes que lo custodia en sus puestos de control en las estaciones o centros de datos toman un café con tranquilidad y comentan el partido del fin de semana. Miran pantallas con gráficos de colores que les muestran el tráfico de datos en una ciudad, en la otra, a las 2.53 de la madrugada, a las 5.38 de la tarde, y así a cada minuto, 365 días, 24 horas. Porque, a pesar del orden y la concentración, la amenaza siempre asoma. Un corte de energía, el ancla de un barco, un terremoto, una grúa que levanta la nieve o una ardilla con ganas de afilarse los dientes pueden dañar los cables y, de repente, poner en peligro nuestras vidas conectadas. Cuando eso ocurre, las alarmas suenan y ellos actúan.

La mayoría de las veces salir a reparar las autopistas informáticas es cuestión de rutina y todo vuelve a la calma rápidamente. Pero hay ocasiones en las que no es tan fácil y las reparaciones dejan a mucha gente sin conexión. Sí: a veces sucede. En el verano de 2014, las construcciones de rutas y estadios para el Mundial de Fútbol en Brasil, sumadas a las *escolas do samba* inmensas cruzando caminos, desataron una serie de cortes en Río de Janeiro y San Pablo durante meses. En 2011, una señora de 75 años que buscaba cables de cobre para vender en el mercado negro en la república de Georgia, en el límite entre Europa y Asia, se topó con un tendido subterráneo de fibra óptica, lo rompió y dejó a toda Armenia —el país vecino— sin conexión por doce horas. A principios de 2008, otro imprevisto: un cable se rompió en el canal de Suez y afectó a 60 millones de personas, desde India hasta Egipto.

—La mayoría de los cortes son por factores humanos. Cosas estúpidas. Pero son las que te pasan.

Desde hace catorce años, Curci sale todos los días de la ciudad de Ramos Mejía, en el Gran Buenos Aires, y llega al barrio de Olivos. Y allí se desploma en su escritorio de Level 3, una de las dos empresas (junto a Telefónica) dueñas de cables submarinos que conectan a la Argentina con internet y dueña también de la red de fibra óptica más grande del mundo, capaz de gestionar por sí misma el 72 % de las direcciones de internet del planeta. Otros días, le toca viajar por las estaciones de cables de América Latina, desde la enorme estación de Miami a la modesta de Las Toninas, para asegurarse de que internet funcione, que los datos corran tranquilos,

como él, cuando luego de trabajar se sube a la cinta del gimnasio a descargar la tensión del día.

—Me ves tranquilo pero tengo úlceras y una gastritis espantosa. En este momento tengo un corte en algún lugar de Buenos Aires, pero es como te decía: si me pongo nervioso yo se cae todo.

De esa paciencia también depende internet. Nos parece automática cuando saltamos de una página a otra pero, en realidad, es una cadena de decisiones tomadas por seres humanos, personas de carne y hueso.

—Para muchas cosas hay procesos automáticos: una pantalla que te indica hacia dónde se enrutaron los datos. Pero a veces hay que hacer las cosas a lo bestia, como antes: tener el mapa en la cabeza y elegir el camino.

De los cuatrocientos hombres que integran su equipo, Curci tiene un grupo de cuarenta que trabaja *solo* en pensar hipótesis de crisis. El famoso «¿qué pasaría si…?». Cada día ellos despliegan tantos mapas como posibilidades de cables rotos existan y entregan un plan detallado con los pasos a seguir ante esa situación: cuánto combustible extra se necesitará para los grupos electrógenos, cuánta comida para los operarios que reparan los cables, cuántos repuestos hay que tener listos en los depósitos para que los barcos de reparación solo tengan que pasar a buscarlos y reducir el tiempo del arreglo. Si algo ocurre, solo hay que recurrir al plan correspondiente y seguir sus pasos. Desde revueltas políticas hasta golpes de Estado, pasando por vandalismos y robos de cables para vender cobre, hasta las cosas más simples, como el golpe de una grúa de nieve, un ancla o un animal curioso con hambre, todo está escrito en un mapa. Estos guardianes imaginan escenarios, a veces causados por pájaros que picotean cables aéreos.

—A mí no me divierte que me rompan un cable —dice Curci—. Pero me obliga a ser rápido, a ver cómo giro el sentido del tráfico para no afectar a los clientes. Me gusta eso. De hecho, cuando no me pasa, me pongo a pensar qué pasaría si mañana tuviera un corte. Me siento con mi gente y les digo: «¿Qué hacemos si se nos corta un cable en el medio de la final del Mundial de Fútbol? ¿Y si mañana hay un terremoto en Buenos Aires?».

El 14 de noviembre de 2007, tuvo que recurrir a uno de esos planes.

Pasadas las tres de la tarde, un terremoto devastó el norte de Chile, desde la ciudad de Tocopilla hasta la capital, Santiago. Los tubos de internet de su empresa estaban en peligro. La conexión de sus clientes, amenazada. Sin pensarlo dos veces, Curci juntó las cosas de su escritorio y puso en marcha el protocolo. Mandó un *mail* a todas las oficinas del mundo declarando oficialmente el problema, reunió a su equipo para desplegar el operativo y dejó su escritorio en Olivos para subirse a un avión con destino a Mendoza.

Con todos los vuelos a Santiago cancelados, el ingeniero cruzó la Cordillera en auto. Cuando llegó a la capital, vio puentes apilados sobre calles y edificios que caían hacia adelante, como piezas gigantes de dominó, sobre autos y carteles. Pero no se

detuvo. El temblor ya había cortado internet durante una hora, casi el doble de los 33 minutos anuales de desconexión que su empresa garantiza a sus clientes.

El ingeniero Curci respiró y se propuso que el temblor no dominara también su mente y su pulso. Sacó la vista del desastre y recordó lo que le decía su madre cuando era un niño: «El que se enoja pierde». Los cuatro días siguientes, mientras los equipos de rescate trabajaban en las calles y los aviones de ayuda cruzaban el cielo, se encerró en un inmenso edificio blanco, un centro de operaciones de la Red —uno de los corazones de la bestia desplegado en el mundo—, y no salió de allí hasta que el servicio volvió a la normalidad. Sus hombres se extendieron como una legión de enfermeros con la orden de coser las arterias rotas para que volvieran a bombear datos, millones de datos. Repararon caños, reconectaron pedazos deshechos de fibra óptica en avenidas con el asfalto quebrado y revivieron los cables de transmisión submarinos atrapados por las placas tectónicas del Pacífico.

—Sí, reconozco que me gusta la adrenalina —confiesa Curci, siete años después de aquel terremoto, mientras recorremos otro de los dominios de su reino de internet: la estación de amarre de cables submarinos de Las Toninas.

Hoy no hay crisis pero sí una tormenta de verano que dejó a los turistas sin playa en plena temporada. La lluvia de enero apenas nos deja ver el puente negro con letras blancas que da la bienvenida al pueblo. Solo hay que doblar para ver la estación. Pintada de amarillo huevo, en forma de herradura y rodeada de muros grises, contrasta con las calles descuidadas, embarradas por el agua. La estación es grande. Ocupa toda una manzana. Pero pasa desapercibida. No es casualidad. Adentro, en una sala común y pequeña custodiada por complejos sistemas de seguridad, vive uno de los tres cables que conectan a la Argentina con internet a través del océano Atlántico. Por ese cable pasa gran parte de los datos de internet que intercambiamos a diario.

Para los 18 integrantes del grupo de Facebook «Las Toninas, capital de internet de la Argentina» la estación es un centro estratégico del país todavía desconocido desde que se instalaron los cables. Esta selecta logia de las redes sociales —que también reclama que eximan al pueblo de pagar por el acceso a internet— todavía sostiene que estamos en el punto exacto donde caería la bomba de la próxima Guerra Mundial. Si eso pasara ahora, tendríamos que salir a la lluvia con pilotos y botas a defender este gran barco donde viven los cables. Pero por el momento la única amenaza real es generada por unos animalitos verdes del tamaño de una mano.

—¡Cuidado con las ranas! —grita desde adentro Raúl De Pedro, jefe de la estación y uno de los tres ingenieros que trabajan en el lugar al mando de Ernesto Curci—. Si venían ayer, con el calor que hizo, estaba lleno de yararás que subían desde la arena. Pero hoy con esta lluvia les tocaron ranas.

Con unos rulos marrones largos que descienden por su rostro hasta transformarse en una barba de meses, camisa a cuadros y *jean* de vestir azul oscuro, De Pedro lleva a los visitantes desde el estacionamiento hasta el interior de la estación. Todo es hermético y seguro, como si estuviéramos en las entrañas del Enterprise de *Viaje a*

las estrellas. En cada pasillo hay señales y carteles de instrucciones ante un eventual accidente; todo está preparado para que el fuego no cruce de una sala a la otra, para que el desastre nunca ocurra y los cables no se corten.

Los cables submarinos de fibra óptica que conectan a la Argentina con internet y con el mundo entran todos desde el océano Atlántico, en Las Toninas, a través de tres estaciones de amarre.

A diferencia de la instalación de la segunda estación que despertó el miedo terrorista en el pueblo, la primera no llamó su atención, tal vez por su modesto tamaño. Fue instalada a una cuadra de la comisaría por la entonces recién creada Telecom Internacional de Argentina en 1994 y albergó al primer cable, que funcionó desde ese año hasta que fue desconectado en 2013. El primer cable submarino de fibra óptica del país, bautizado Unisur, era muy corto comparado con los actuales. Medía solo mil setecientos kilómetros pero su tecnología de transmisión superaba en velocidad y capacidad al cobre y se usaba tanto para datos telefónicos como para los primeros de internet. Su recorrido formaba la figura de un número tres que se posaba sobre Las Toninas en Argentina, Maldonado en Uruguay y Florianópolis en Brasil. Tres años antes, esos tres países, junto con Paraguay, habían firmado el Tratado de Asunción, que ponía formalmente en marcha el Mercosur[5].

Solo seis años antes, en 1988, se había instalado el primer cable transatlántico de fibra óptica del mundo, entre Estados Unidos, Inglaterra y Francia.

—Instalar un cable tan grande es inexplicable —dice Curci, con nostalgia—. Cuando lo inauguramos, no podíamos creer lo que habíamos hecho. A veces cuando lo pienso creo que fui el creador de algo, pero que alguien me dictó el plan de cómo hacerlo.

Tras casi veinte años en funcionamiento, ese cordón umbilical de fibras que sirvió para las primeras transmisiones de internet en el país salió de circulación en diciembre de 2013. Ahora quedó en el Mar Argentino como el fósil de un animal en descomposición esperando a que alguien lo saque del paso y lo transporte a un museo para ser exhibido como un pionero.

Luego del Unisur llegaron tres cables submarinos más. Todos se instalaron entre 1999 y 2000, impulsados por el avance mundial de lo que hoy conocemos como la Red. En Argentina, en el año 2000, el fin de la exclusividad de Telefónica y Telecom para prestar servicios de telecomunicaciones internacionales abrió el mercado a otras empresas que, ya avisadas del proceso de apertura, tenían sus cables listos para empezar a operar. En esos años, la Red local sumó 53 500 kilómetros de cables de fibra óptica —el equivalente a cruzar ida y vuelta de Alaska a Tierra del Fuego— y seis mil millones de dólares de inversiones. Todos sus nuevos tentáculos, pelos, ramificaciones y datos entraron también por Las Toninas, el kilómetro cero de internet en la Argentina.

El 10 de mayo de 2000 se inauguró el cable Atlantis 2. Con 8500 kilómetros, une América, África y Europa. También sale, por supuesto, desde La Toninas, de la

misma pequeña estación de amarre de la que salía el Unisur. Hoy, producto de 14 años de avances tecnológicos, ese mismo cable puede llevar 160 gigabits por segundo (160 mil millones de letras —o números, o números y letras que forman imágenes, conversaciones, videos—). Unos meses después, en septiembre de 2000, comenzó a operar un nuevo cable desde la imponente estación de amarre, cuya construcción había generado tanto pánico: el South American Crossing (SAC). El cable recibió su nombre por la compañía que lo construyó, Global Crossing, comprada en 2011 por Level 3. El SAC, además de un cable, conforma un anillo de veinte mil kilómetros que une América Latina, de este a oeste. Por tierra, se completa con otra extensa red de cables y centros de datos que conforman el *backbone* de la empresa, una columna vertebral de internet capaz de transportar grandes volúmenes de datos que luego se extiende hasta llegar a cada ciudad, cuadra y casa (en Argentina, la empresa tiene centros de datos en Buenos Aires, Córdoba y Mendoza). Level 3, quien sigue operando este cable, es uno de los once proveedores de servicios de internet (ISP) de nivel Tier 1, es decir, que puede gestionar el nivel más alto de conexión y tiene presencia internacional[6]. La forma de anillo de la red no es casual. Permite que, si se corta alguna parte de la red, el tráfico se enrute o dirija al lado opuesto y encuentre caminos alternativos para seguir transmitiendo los datos.

El tercer cable está un poco más lejos, tomando la calle principal de Las Toninas y llegando a Costa Chica. Si bien fue inaugurado en 2001, el edificio parece recién emplazado. Es un rectángulo perfecto de hormigón gris rodeado por un jardín verde y un muro de ladrillos calados. Parece una cárcel de lujo, con un césped cuidado para jugar al golf. El edificio alberga al SAM-1 (South America 1), un cable de 25 mil kilómetros, propiedad de Telefónica, otra de las redes Tier 1 de Argentina, con conectividad directa y propia entre América Latina, Estados Unidos y Europa. El SAM-1 hace lo mismo que el cable de Level 3: recorre América Latina desde Las Toninas, pasando por trece estaciones que conectan por el Atlántico hasta Boca Ratón en Miami, donde retornan por el Pacífico hasta amarrar en Valparaíso, Chile.

Flavio Ferrari, hoy encargado de la estación que cobija al SAM-1, un toninense de 38 años y ojos grandes que sonríe mucho, se sorprende cuando alguien visita su lugar de trabajo, un galpón enorme colmado por *routers* y servidores. La estación, igual que la de Level 3, se pensó más grande de lo que hoy necesitan. Sus servidores, apilados como torres, transportan casi 2 terabytes por segundo, que equivalen a 600 horas de video, 7 millones de fotos digitales o 2 mil ediciones completas de la *Enciclopedia Británica* digital.

En la estación el trabajo es muy limitado, casi un «paso obligado» del cable para cargar energía. Las decisiones más importantes del SAM-1 las toma su estación hermana de Lurín, Perú. Ferrari, hijo de una operadora telefónica, de aquellas mujeres que conectaban las perillas de las comunicaciones internacionales cuando se hacían punta a punta, estudió electrónica y empezó a trabajar unos meses antes de la instalación del cable submarino.

—Fueron cinco días sin dormir, con cuarenta personas trabajando. Éramos cuatro de Telefónica y el resto de Tyco, una empresa suizo-estadounidense que instaló los cables junto con Alcatel —cuenta saliendo del letargo de un día común de enero—. Después trabajamos quince días más para dejar el cable en funcionamiento. Cuando terminamos no sabíamos en dónde estábamos, pero sabíamos que habíamos hecho algo grande. Queríamos dormir, pero nos quedábamos mirando el recorrido, hablando sobre detalles técnicos que todavía no conocíamos bien, pero que suponíamos cómo iban a evolucionar, porque todos estamos en esto hace mucho.

Mientras que la estación de amarre que alberga al SAM 1 y a su guardián Flavio Ferrari está aislada y sobre la ruta, la del SAC, operada por Level 3, se ubica en el centro de Las Toninas. Raúl De Pedro hace de guía por sus pasillos. Carga, honrando a su apellido, las llaves de cada puerta que abre a su paso. Tiene la autoridad de haber cuidado el cable de la estación desde que lo instaló, también él mismo, hace catorce años. Quizá sabe que su vejez será la vejez del cable: que hoy, a sus 50 años, lo vio crecer. Que cuando se jubile el cable seguirá ahí, con alguna reparación, pero funcionando. Esa también será su victoria.

En la «casa del cable» las paredes están pintadas de un gris metálico. Los techos y los pisos relucientes combinan con la luz artificial. Tiemblan ante los pitidos de los sistemas de seguridad de las puertas que va cerrando De Pedro. Los servidores, encendidos las veinticuatro horas, emiten un ruido monótono que se mezcla con el aire acondicionado que lucha contra el calor acumulado de los aparatos y mantiene los espacios fríos, en veinte grados o menos. A las estaciones y también a los centros de datos siempre hay que llevar un abrigo. A más torres de servidores o *racks*, más aire, más lucha de los equipos contra la temperatura de las máquinas *pensando* todo el día. De Pedro, ya acostumbrado a los ambientes frescos, solo lleva puesto una camisa. Lo sigue Marcelo Peresutti, su compañero en la estación, también de su edad pero más flaco, de gestos suaves y voz pausada. Y más atrás, Leandro Vidal, el tercer ingeniero que cuida el cable. Recién recibido, más joven y callado, los asiste con esmero hasta llegar a la sala maestra, donde se encuentra *él*, la estrella: el famoso cable de internet.

De Pedro abre la puerta de una habitación de dos metros por seis. Nada indica que allí haya algo valioso. Cuesta creer que internet *sea* simplemente un cuarto con dos cables negros, el que transmite los datos y el que le da energía. Cuesta creer que para estar de pie frente a ellos tuve que esperar meses, decenas de llamadas, discusiones con agentes de prensa, presentación detallada de datos personales y autorizaciones con abogados corporativos de la compañía.

Pero *él* está ahí y toda aquella burocracia ya no importa: el cable, un tubo negro de tres dedos de ancho, apenas más grueso que uno doméstico, tiene pegada una advertencia que avisa «Alta tensión». Como todo objeto de deseo, se puede mirar, pero no tocar. Es uno de los corazones del monstruo de internet, la parte que lo alimenta, lo ilumina y lo hace cumplir su función de transportar información. Por allí

pasa gran parte de la subjetividad moderna: *mails*, posteos de blogs, fotos de redes sociales, archivos de música y películas que intercambian ingleses con argentinos, suecos con coreanos, brasileros con rusos. A su lado, el cable tiene otro tubo, encargado de darle energía y cerrar el circuito de corriente eléctrica.

Cuando se corta un cable, terrestre o submarino, la forma de detectar el punto exacto de la rotura es a través de señales eléctricas: cuando encuentran una barrera, allí está el problema. Una vez detectada la falla, los técnicos (o buzos si es en el mar) reemplazan la parte cortada, siempre un tramo ínfimo comparado con los miles de kilómetros del cable. Por eso en esta estación, como en las otras *landings* o centros de datos, la provisión de energía eléctrica es fundamental. Afuera del edificio pero dentro de los muros, se pueden ver los tanques de gasoil preparados para alimentar a los grupos electrógenos y una doble sala de baterías. El suministro debe ser permanente.

—La hipótesis de crisis extrema sería quedarnos sin combustible para los grupos electrógenos —dice De Pedro—. Tenemos energía para funcionar una semana. Tendrían que cortar todas las rutas durante siete días para generar un problema.

Con esa afirmación explica también por qué, más que una bomba, la herida mortal para los cables y la bestia sería un corte de electricidad.

De Pedro le pide a Leandro, su asistente, que traiga un tramo de cable de fibra óptica submarino de diez centímetros, entregado como *souvenir* de visita. Fuera de esta estación, el cable sería un cable de plástico más, con capas que forman un cilindro de casi cuatro centímetros. La primera, más ancha y negra, está en contacto con el agua y soporta su peso. Luego hay aislantes verdes, capas de cobre conductoras de electricidad y jirones de acero que protegen al cable de roturas. Al final, en el corazón del tubo, asoman unos pelitos de fibra óptica. Son muy suaves y están pintados de unos colores estándar usados por la industria de telecomunicaciones: amarillo, azul, verde, naranja, marrón, rosa. Su componente principal es sílice, estirado cuidadosamente hasta formar un vidrio alargadísimo, tan fino que se mide en micrones[7]. Un mito repetido en la industria dice que clavarse un pelito de fibra en el dedo puede causar la muerte. ¿Será verdad?

—Sí, si te entra un pelo de fibra al torrente, tiene el mismo diámetro que un capilar sanguíneo y te podés morir —confirma De Pedro—. Yo no sé si es 100 % verdad. Pero por las dudas nosotros acá nos cuidamos.

Los cables submarinos son mucho más gruesos que los terrestres. Y son más gruesos cuanto más cerca de la costa están, para resistir la actividad humana que pueda dañarlos. También porque es allí donde están enterrados a la menor profundidad de todo su recorrido, a un metro y medio. Pero en la playa no hay nada que señale que el cable está ahí.

—Es por seguridad —se ríe De Pedro—. Si pusiéramos un cartel para señalar el cable, la gente iría a buscarlo, a tocarlo, a romperlo, a ponerle una bomba.

Desde el mar a la estación, el cable sigue extremadamente protegido por un camino cubierto de capas de hormigón y terrenos cercados. El recorrido secreto solo lo conocen Curci, De Pedro y algunos hombres más. Son un selecto grupo de guardianes de una bestia condensada en un cable de dimensiones demasiado terrenales, frágiles. En Las Toninas son también tres hombres los que tienen ese mapa de 18 cuadras en la mente, y una vez al día uno de ellos cumple con la tarea de salir de la estación y caminar sobre los pasos del cable.

Una vez que llega, funciona en base a dos procesos tan distintos como estéticamente complementarios: cantidades astronómicas de electricidad y procesos ópticos refinadísimos, algo así como una radiografía que te permite chequear que lo que estás transmitiendo sea lo que querés transmitir. Internet se alimenta de ellos y los necesita. Pero ambos procedimientos avanzan tan rápido en la industria de las telecomunicaciones que, en las estaciones de Las Toninas (y en cualquiera del mundo), con la misma cantidad de tubos y pelos de fibra instalados en el 2000, hoy se transmite un 400 % más de datos que cuando se instalaron las estaciones. Dentro de un año ese volumen podría pasar a un 5000 % más. Esos saltos de tecnología hicieron que esta y las otras estaciones de amarre quedaran gigantes, como supermercados llenos de góndolas vacías esperando a un repositor que se quedó dormido. Hoy, en estos salones blanquísimos y asépticos, podríamos estar festejando tres casamientos —uno en cada sala con la música a tope; la aislación lo permitiría— y, al mismo tiempo, desde otra sala, seguir trabajando.

En el techo, las bandejas color naranja sostienen otros cables, los que conectan a los servidores con la electricidad externa. Una zapatilla de enchufes cae desde arriba y conecta un cable a 220 voltios. En una de las mesas, frente a un mueble con torres de servidores, una computadora Toshiba Tecra 8100 resiste desde la inauguración de este cubo de cemento, en el año 2000, conectada para hacer pruebas de señal. Es la típica laptop ladrillo, pesa más de cinco kilos y en el sitio de ventas *online* Mercado Libre la venden como antigüedad tecnológica para fanáticos a 160 pesos. Pero aquí, arriba de una mesa perdida en el centro de una sala gigante de la estación, cumple una función estética: es el elemento de ciencia ficción que faltaba al paisaje. La máquina sirve para apretar un botón, una vez por día, y chequear que el mundo de internet esté funcionando correctamente. Vive allí desde hace quince años y hace también quince años que solo cumple con esa operación. El avance tecnológico se dio en lo más pequeño, en la parte más fina, casi invisible: la fibra óptica. El resto de los aparatos que la rodean —y sus guardianes— no han cambiado. Las Toninas, allá afuera, también permanece igual.

Es enero y la temporada viene mal, se quejan los comerciantes. Las Toninas es un lugar venido abajo, con veredas desparejas, baches en las calles y carteles

despintados. Entonces, ¿por qué decidieron poner los cables de fibra óptica submarina justo acá?

—Las Toninas es un lugar plano, con pocos accidentes, con pocos barcos, donde es fácil obtener permisos para construir, negociar límites marinos y estar cerca de otros cables.

Pero además de las razones geográficas hubo un motivo económico, también de pueblo pequeño, que definió a Las Toninas como el lugar elegido. Aquí, en la Capital Nacional de Internet, no hay puerto. Los barcos se fueron quedando en San Clemente, la primera ciudad del Partido de la Costa que se ve en el mapa viniendo desde Buenos Aires.

Si bien estamos en el hogar de los cables de internet, la banda ancha y las conexiones rápidas no abundan. En el centro, el complejo de departamentos Tony Center ofrece internet a 15 pesos la hora. En la otra cuadra, sus mismos dueños tienen un bar, con un *router* más potente e internet *wifi* a la que se accede con una clave al tono: *soyarenaymar*. En las vidrieras hay animales marinos hechos de caracoles, lata y madera. Uno igual a otro, todos con corazones, todos «I <3 Las Toninas», con palmeras que no existen en Las Toninas. Además del locutorio, los turistas pueden conectarse a internet comprando unos papeles rojos y negros envueltos en celofán que la cooperativa de la zona, Atlántica Video Cable, llama «tarjetas prepagas». Retirado el celofán, un portal con publicidad de Mundo Marino pide el código de la tarjeta y se puede navegar a una velocidad que hubiera sido buena en 1998 y hoy abre las fotos en tres minutos. Para los cinco mil habitantes fijos del pueblo, las opciones son las mismas que para la mayoría de Argentina: las monopólicas Telefónica y Cablevisión, y la cooperativa de Pinamar Telpin. Las Toninas es más bien un puerto pasajero de cables, donde cargan energía para seguir hacia el resto del país. Desde aquí, los cables siguen por tubos enterrados en paralelo a la ruta 11 y van yendo hacia el norte, hasta llegar a Buenos Aires y ramificarse por toda la Argentina.

Para que la señal conserve su intensidad en todo el recorrido se instalaron los repetidores, unas cajas que se conectan de un lado al otro del cable. Desde Las Toninas hasta la estación de Santos, en Brasil, hay 2000 kilómetros y 32 repetidores debajo del mar. Lo mismo ocurre cuando el cable sigue por tierra. Desde Las Toninas a la capital argentina, hay un repetidor cada 100 kilómetros: Conesa, Cerro, Verónica, La Plata, Buenos Aires. Hacia el norte, hasta llegar a Salta, hay 30 repetidores más que acompañan los cables terrestres.

Antes de la fibra óptica, se lanzaba una señal y se esperaba que, del otro lado, alguien respondiera. Si no había respuesta, se intentaba otra vez. Así hasta que llegaba el mensaje. Hoy los datos, las imágenes, la voz, corren al mismo tiempo por una misma fibra, donde además circulan otras señales. La información siempre llega.

Sin embargo, todavía hay tareas que la tecnología no reemplaza. Instalar un cable de fibra óptica submarino es un trabajo descomunal. Los avances técnicos no suplieron la gran operación humana que se necesita para subir rollos de miles de

kilómetros de cable a la bodega de un barco, enterrarlo mil metros saliendo de la costa y luego completar el tendido en el fondo del mar respetando una ruta precisa y previamente definida. Para lograrlo se necesita casi lo mismo que en 1850, cuando se instaló el primer cableado entre Gran Bretaña y Francia a través del Canal de la Mancha: un barco, marineros, días sin dormir, mucha fuerza, algunas órdenes, un par de gritos. Y paciencia. De la que da el mar y de la que hay que inventar cuando el viento, las olas o el empalme del cable no ayudan a terminar y volver a casa.

El 95 % de las comunicaciones del mundo se hace a través de redes de fibra óptica que corren bajo el mar y unen los continentes por los océanos. Los cables son más de 250 y unen casi un millón de kilómetros, lo que equivale a 22 vueltas al mundo. Para que eso suceda, son necesarios ejércitos de hombres en barco que invaden costas y enchufan la tierra con el mar.

José María Vázquez coordina uno de esos equipos que pasan su vida en el mar. Su empresa, Dynamic Marine, instala y repara cables submarinos. En 2011, él fue parte de la expedición que instaló el Bicentenario, un pequeño cable de 250 kilómetros que une Las Toninas con Maldonado[8], Uruguay.

Emplazar un cable también es un acto burocrático inmenso. Cada instalación o reparación requiere una serie de permisos de organismos como Cancillería y Prefectura, a quienes se debe presentar el mapa exacto del recorrido para que el Servicio de Hidrografía Naval lo asiente en las cartas marítimas, actualizadas periódicamente. Una vez asentado el cable en el lecho y publicado en la carta marítima, nadie puede pescar ni hacer obras en su «zona otorgada» sin pedir autorización previa. Aun así, las roturas por pesqueros furtivos, generalmente de noche, son comunes y el motivo más frecuente de fracturas de cables submarinos. Para evitarlo, las empresas de telecomunicaciones están trabajando hace unos años con las Naciones Unidas en las Conferencias sobre el Derecho del Mar, para avanzar en una mayor protección de los cables. El objetivo es declarar a internet un «servicio universal esencial» de la humanidad —sin conexión se pierde gran parte de la actividad y la generación de riqueza diaria— y a partir de esa categoría generar normas mundiales que protejan a los cables de las roturas o castiguen más severamente a quienes las produzcan.

Resuelta la burocracia marina, el barco cablero puede partir. La mayoría de ellos son de dos empresas: la francesa Alcatel y la norteamericana Tyco. En ellos, uno de los costos más altos es el del personal especializado que hace la instalación del cable y lo deja en funcionamiento.

—Las mismas empresas que fabrican el cable submarino te mandan el rollo ya diseñado según su ruta y un técnico especializado que lo instala. Solo está autorizado a hacerlo él. Es como un gasista matriculado, pero de fibra óptica.

Vázquez conoce a muchos de estos expertos, que en general hablan el francés de Alcatel o el noruego de Nexans, algunas de las marcas más usadas en la industria.

—Son estrellas de *rock*: van todo un mes en el barco pero por ahí solo trabajan dos horas, cuando el cable ya está listo y tienen que dar el OK.

Su tarea es coordinar todas las tareas de un barco, durante semanas, hasta que la compañía que lo contrata le confirma que el cable está transmitiendo y puede volver a casa.

—Es difícil. Pero lo más complejo es que cuando llega el momento del empalme, el momento clave, el técnico esté sobrio. Mi trabajo, más que técnico, es conservar la armonía. Son gente que toma mucho.

Tras la confesión, Vázquez se anima a derribar otro mito: el que dice que los tiburones se comen los cables submarinos y son responsables de muchas de las roturas de fibra marina. En 1987, en su artículo «Los ataques de tiburones retrasan la instalación de cables submarinos de fibra óptica», el *New York Times* alertaba que estos peces «sienten una atracción hasta ahora inexplicada por los nuevos cables submarinos de comunicaciones que preocupa a las empresas propietarias e instaladoras». El texto comentaba que habían ocurrido ataques en los océanos Atlántico y Pacífico, que habían «dado lugar a una ola de interés por el comportamiento de los tiburones y hasta el descubrimiento de nuevas especies». Según afirmaba James Barrett de AT&T, una de las instaladoras, habían hallado dientes de estos enormes peces en un tendido en las islas Canarias. «Nos vimos sorprendidos», comentaba el ingeniero.

El problema de los tiburones efectivamente existió. La propia AT&T destinó millones de dólares a investigar el misterio. Finalmente, se llegó a la conclusión de que lo que les gustaba a los tiburones no era el cable en sí ni la sensación de afilarse los dientes contra él. Vázquez tiene la respuesta:

—Los tiburones confundían la corriente eléctrica que emite el cable con unas ondas similares que generan los peces. Entonces, pensando que el cable era un pez, es decir, comida, lo mordían. Esto se descubrió desconectando el cable: si no tenía más corriente, el tiburón seguía de largo, ya no le interesaba.

Tras los estudios, la solución de la industria fue tan sencilla como agregar otra capa a los cables submarinos. Los grandes peces dejan de pensar que el cable es comida y el problema está resuelto. Las crisis, ahora, ya no están bajo el agua, sino en la superficie, cuando los cables suben y se enfrentan con los verdaderos generadores de problemas: los seres humanos.

II

Las telecomunicaciones en Argentina, de Sarmiento a De Vido

> «Solo podemos hablar de estar conectados como de un estado mental porque damos por sentadas las conexiones físicas que nos permiten estarlo».
>
> ANDREW BLUM.
> *Tubos* (2012).

Una mañana de mayo de 2014, hace un año, mi proveedor de internet decidió mostrarme su poder.

Tras un viaje abrí el *mail*, intenté borrar rápido el *spam* de la madrugada para responder lo importante, mientras abría varios sitios de noticias a la vez para volver al mundo. Sin embargo, algo se interponía. Las páginas se quedaban tildadas, formando unos círculos que giraban pero no se decidían a cargar. Le eché la culpa a mi ausencia: seguro que durante ella un corte de luz había desconfigurado el módem. Lo desenchufé y lo volví a encender. Pero nada. De repente, se interpuso una pantalla blanca que me pedía pagar *online* mi servicio de 10 megas y aprovechar una promoción para comprar espacio en la nube y guardar muchísimos megas más, aunque esa mañana ni siquiera me podía conectar. Era obvio: mi proveedor se estaba metiendo conmigo.

Llamé al servicio técnico. Con amabilidad de manual, Diego, el operador, me guío por los chequeos de rutina. Me hizo reiniciar el módem y en menos de tres minutos me informó que el problema estaba solucionado. Mi furia de usuaria estaba más calmada, pero mi oficio de periodista quería una respuesta. Después de cinco preguntas, Diego se cansó y me dijo la verdad: «Tenías atascado un paquete de publicidad en la línea». Tal vez agotado de mentirle a los clientes, me dijo que mi proveedor, Telefónica, quería promocionar un nuevo servicio y hasta que el cliente no hacía clic para verlo (algo que yo no hacía), la publicidad insistía en aparecer y bloquear la navegación. Seguramente, Diego no sabía que yo era periodista y estaba escribiendo un libro sobre internet. No se lo dije, pero yo lo sabía: la empresa, como dueña de los caños y los cables, podía meterse con mi conexión, mis megas y mi paciencia. Era técnicamente capaz de hacerme ver lo que quisiera (aunque, por supuesto, eso no era ético). Tampoco le dije nada de eso. Le agradecí por su tiempo y lo califiqué con un 10 en la encuesta de calidad de la llamada en agradecimiento a su falta de confidencialidad con los secretos de su empleador.

Pero no sirvió. Durante un año, una vez al mes, la pesadilla se repetía. Como en la película *El día de la marmota*, en vez de despertarme el mismo día una y otra vez, mi tragedia era que internet se atascaba. Lo mío no era un mal sueño. Yo sabía por qué pasaba.

Las empresas nos hablan de internet como una nube de ondas que atraviesan el aire, de hilos que nos cruzan por todos lados y llegan a nuestra computadora o teléfono cuando necesitamos un camino libre para mandar un *mail* o descargar una foto.

Pero la internet *real* es distinta. Está hecha de conexiones físicas y sociales muy concretas. Los hilos por donde viajan los bits se pueden tocar. Son tubos, caños, edificios. Son lugares, en medio de la ciudad o en galpones alejados, donde la información entra, se interconecta, se ordena, se empaqueta y sigue viajando. Y los manejan personas: los dueños de las empresas, sus empleados, sus accionistas. Internet está hecha de lugares con pasado, con sonidos, colores y olores, con hombres —y pocas mujeres— que instalan y reparan aparatos. Cada vez que lanzamos algo a la Red —subimos, posteamos, comentamos, retuiteamos, etc.— estamos alimentando a ese monstruo, como proteínas en forma de bits: una letra, un número, un pixel que va por algún cable, se cruza en algún servidor o queda alojado en otro. Porque los recorridos de internet también son reales. Si quisiéramos trazar la ruta de nuestra información, solo necesitaríamos de un papel para anotar las coordenadas geográficas de los caminos. Luego, esos puntos unidos nos darían un dibujo situado en lugares reales. Su infraestructura siempre está cerca de nosotros.

¿En qué cambia para nosotros saberlo, si solo nos interesa conectarnos? ¿Por qué habría de interesarnos ese mapa mientras internet funcione? «Si no está roto no lo arregles», dice una frase muy citada en el mundo de la tecnología y de internet[9]. Sus defensores técnicos señalan que mientras todo marche bien no hay que «tocar» nada. Sin embargo, esa idea es engañosa y esconde muchos riesgos para nuestro futuro.

Conocer el mapa de internet y su funcionamiento es conocer el territorio que habitamos.

La tecnología está presente en cada acción de nuestra vida: los saludos de cumpleaños. La petición política que firmamos virtualmente desde el sofá. El video de gatitos más visto de la semana. La búsqueda de un dato sobre una empresa poderosa. El perfil de nuestro próximo empleador. Todo eso que buscamos y hacemos pasa por el entramado físico instalado y controlado por unas empresas que no vemos, pero que están allí. Nos resulta más cómodo suponer que el chat que deslizamos con el dedo hacia abajo en la pantalla *touch* del celular se diluye en el aire, que el video que terminamos de ver se desvanece cuando cerramos la pestaña, que el perfil que analizábamos con precisión de detective nunca supo que estuvimos allí. Pero nuestras huellas quedan en cada cable y en cada servidor de un grupo de empresas. Ver el video de gatitos, hacer un curso *online* o compartir nuestras fotos son la parte del

iceberg que vemos, pero que en su base se sostiene por grandes corporaciones, leyes y *lobbies*.

Internet se basa y se nutre de confianza: la de las redes que se unen para transportar la información y la nuestra, hacia las empresas que transportan esos datos. Nos preocupamos por averiguar quién va a cuidar a nuestros hijos o el estado financiero del vendedor de nuestro próximo auto. ¿Por qué entonces no nos preguntamos acerca de las empresas por donde pasan nuestras vidas digitales?

En la Argentina, el 65 % de los habitantes usa internet**[10]**. Para conectarse, 8 de cada 10 personas podemos elegir entre los tres proveedores que dominan el mercado: Speedy de Telefónica, Arnet de Telecom y Fibertel del Grupo Clarín. Con 1,8 millones, 1,7 y 1,6 clientes, respectivamente**[11]**, las tres compañías conforman un oligopolio que deja poco lugar a la competencia. El 78 % de los argentinos conectados se agrupa en el 30 % del territorio: Capital Federal, Buenos Aires, Córdoba, Santa Fe y Mendoza. Estas cinco provincias, las más habitadas y con mayor rentabilidad para ofrecer servicios, forman un «anillo» donde conectarse a internet es más fácil (en general, hay varias opciones para elegir) y donde existe una calidad de conexión superior a la del resto del país**[12]**. Las empresas más pequeñas se encargan del resto del mapa y llegan a los lugares que «las grandes» no alcanzan, porque hay menos habitantes y, por lo tanto, menos clientes. En estas áreas, conectarse a internet es más caro, el servicio es de muy baja calidad o directamente no hay cobertura.

Además de la concentración en pocos proveedores y la centralización geográfica, en Argentina internet es lenta y cara, comparada con la de América Latina y el mundo. La velocidad promedio de conexión del país es de 5 megas por segundo, casi 4 veces menos que el promedio mundial de 18. En comparación regional, es menos de la mitad de los 9 megas que ostenta Uruguay, los 11 de Brasil y los 12 de México. La distancia se acrecienta frente a los 24 megas promedio de Estados Unidos y Rusia, los 47 de Suecia o los 53 de Corea del Sur. La velocidad promedio de la internet local es comparable a la de Perú, Libia y Angola. Aun así, la baja calidad no implica que sea más barata**[13]**. Argentina tiene uno de los precios de internet más caros de la región**[14]**, solo superado por México, otro de los países con un mercado altamente concentrado, dominado por el monopolio Telmex de Carlos Slim, el segundo hombre más rico del mundo, después de Bill Gates.

Cada centímetro de internet tiene dueño. Somos ciudadanos de esos territorios conformados por cables, servidores, direcciones, redes sociales, aplicaciones. Si después de saberlo igual aceptamos seguir en ellos, tal vez lo haremos por otras razones: porque no hay otra opción, porque es más cómodo, porque es más barato. La diferencia es que ya no será desconocido. Después de saber, mirar para otro lado será elegir, o aceptar pero sabiendo en qué lugar de ese mapa estamos parados.

No obstante, además de ubicarnos hoy, conocer el mapa es vital para el futuro. Porque la Red no está en paz. Porque en ella sucederán gran parte de los conflictos de los próximos años: la lucha entre proveedores de tránsito (quienes nos conectan) y

contenidos (las empresas que manejan los datos) por la neutralidad de la Red; la guerra por la libertad de expresión que ahora tiene un nuevo campo de batalla en las nuevas plataformas *online*; los conflictos entre monopolios y creadores por los derechos de autor; la pugna entre usuarios, empresas y gobiernos por el control de los datos personales y la privacidad; internet y la tecnología utilizadas como arma de vigilancia global de los ciudadanos. Saber quiénes son sus dueños, qué parte opera cada uno y cómo llegó a ocupar su lugar de poder nos permitirá entender las guerras que vienen y cómo defendernos en ellas. No entender esa cartografía es vivir en una habitación oscura. Pero conocerla es más sencillo de lo que parece. Y no siempre el secreto que prima en las cuestiones de la tecnología es conspiración de las empresas. A veces se trata de no habernos hecho algunas preguntas elementales. ¿Qué camino recorre nuestra vida digital cada día?

Los empleados del kiosco de la avenida Corrientes y Paraná, en el centro de la ciudad de Buenos Aires, atienden de a dos. En cada esquina de la gran avenida donde vive el Obelisco, los teatros, los estudios jurídicos y las librerías, hay un local igual al otro. Durante 24 horas, dos chicos de veintitantos años se hacen compañía para dar abasto en las horas pico. Ahora, con el sol después del almuerzo, la dupla de kiosqueros descansa. Se sientan de costado en unas banquetas altas y chequean sus notificaciones de Facebook en el celular. Uno le muestra al otro la chica que quiere invitar a la salida del turno a tomar algo a la noche. Se intercambian los celulares, se muestran un chat de WhatsApp.

—¡No! ¿Qué hacés? ¿Cómo le vas a decir eso? Te rezarpaste —se queja el más chico, de buzo a rayas.

Su compañero se ríe y vuelven a cambiar los teléfonos.

Ellos no lo saben, pero están parados sobre el monstruo de internet.

De pie en esta esquina de la ciudad, mirando hacia abajo, el recorrido de internet deja de ser invisible. Las redes que los empleados del kiosco usaron para mirar sus fotos y mandar el mensaje están aquí, debajo de sus pies y de los míos. Con la vista en el asfalto, el mapa de las conexiones emerge ante los ojos. Como Alicia en el País de la Maravillas, pisar las baldosas desde la esquina del kiosco, pasando por uno y otro mojón hasta el negocio de camisas para abogados a mitad de la cuadra, es recorrer la historia de las comunicaciones en Argentina. Aquí pasan desde los cables de teléfonos a las conexiones internacionales y se puede seguir incluso la historia de las compras y fusiones de las empresas hasta llegar al mapa actual.

Sobre la calle pisoteada de taxis vacíos y colectivos viejos, hay una tapa redonda. Decorada con hexágonos pequeños, tiene la marca de Entel, la exempresa telefónica estatal, luego privatizada y convertida también en proveedor de internet a través de Telecom y Telefónica. A su lado, una doble tapa rectangular señala que por esa misma calle pasaron instalaciones de Impsat, una de las primeras empresas argentinas

que prestaban servicios de comunicaciones e internet al exterior, parte del Grupo Pescarmona y adquirida en 2006 por la multinacional Global Crossing (luego a su vez comprada por Level 3). Subiendo la vereda están las compañías de internet. Telecom —un rectángulo con un logo en medialuna— y Telefónica —una tapa más pequeña con su nombre en letras redondeadas— son las dos compañías telefónicas que tienen presencia de internet en todo el país, al que se dividieron en zonas de operación tras la privatización de 1990. Entre las dos, hoy tienen casi el 60 por ciento del mercado a través de sus proveedores Speedy y Arnet. El tercer proveedor con más abonados, Fibertel, acapara casi el 25 por ciento de los usuarios, que se conectan a través de su servicio de internet y televisión por cable. Debajo de nuestros pies, en esta vereda, también está su marca: son las tapas plateadas que dicen CV, las siglas de Cablevisión, la empresa de cable de la compañía y su nombre legal. Un poco más cerca del subte y de la entrada de algunos edificios, pueden verse las cubiertas metálicas de dos empresas más pequeñas, que prestan servicios en la ciudad y algunos centros urbanos del país: Metrotel, señalada con un adhesivo azul y celeste, e Iplan, oculta bajo su nombre legal: NSS (por los apellidos de sus fundadores: Nofal, Saubidet y Stewart). Ya más lejos, una gran tapa revela con un círculo a rayas un nombre conocido internacionalmente: AT&T, que tuvo una presencia importante en Argentina hasta 2004[15] y actualmente presta servicios corporativos de transmisión de datos y se prepara para crecer en un segmento de gran potencial futuro: la banda ancha móvil.

En el futuro, los arqueólogos podrán mirar el suelo de esta esquina y descubrir las capas de la historia de la Red. Internet está aquí, a la vista, con la condición de querer verla tan simple como puede ser: cables y aparatos conectados entre sí. Sin embargo, su recorrido comenzó mucho antes que esta foto y le agrega el desorden de un animal que fue mutando. Internet está hecha de capas, al igual que la ciudad. Pero además, las capas de la Red, como las de la metrópoli, fueron mutando y reflejan, aún hoy, otros cambios: los de la sociedad, la economía y el poder, y de los hombres que decidieron su crecimiento y su forma. A través de esa historia también se construyó el mapa.

El miércoles 5 de agosto de 1874, a las dos de la tarde, el presidente Domingo Faustino Sarmiento inauguró en la Casa de Gobierno las comunicaciones internacionales de la Argentina con Europa a través de un cable de telégrafo transatlántico. La conexión unía Buenos Aires y Montevideo, subía hasta Brasil hasta llegar a Pernambuco. Desde allí cruzaba el océano Atlántico hasta Lisboa. El día fue feriado y en la tapa del diario *La Nación*, bajo el título «Gran fiesta nacional», se leía: «La República se halla desde hoy al habla con todos los países del mundo civilizado. De hoy en adelante, las pulsaciones del pensamiento humano podrán repercutir, casi simultáneamente, en todas las naciones de la tierra. ¡Gloria al progreso y a la

civilización de nuestro siglo!». Sarmiento, el mayor impulsor del invento, decía que, a partir de ese día, los pueblos alejados comenzaban a convertirse en «una familia sola, un barrio». Sus palabras eran, 115 años antes de la aparición de internet, una premonición de la idea de la Red, de «la gran aldea» de seres humanos comunicados sin importar su ubicación en el mapa.

Con el telégrafo y con cada salto tecnológico que afectó las comunicaciones modernas se produjeron dos cambios simultáneos. El primero es el cambio del invento «en sí», el que afecta tiempos y espacios. El segundo son las instituciones y relaciones sociales, y las formas de pensar que ese cambio lleva consigo. Como decía el teórico cultural Raymond Williams[16], lo que altera nuestro mundo no es el medio de comunicación en sí, sino los usos que le da cada sociedad, que va adoptando tecnologías y prácticas de forma complementaria, superpuesta, conflictiva. Así sucedió desde el telégrafo a internet.

El telégrafo producía un cambio tecnológico vital: el tiempo le ganaba al espacio. Por primera vez en la historia de nuestra especie, los mensajes podían ir más rápido que lo que se tardaba en llevarlos de un lado al otro. Sarmiento había sido testigo, en 1847, de los primeros tendidos de líneas telegráficas en Francia. Unos años después, como embajador en Estados Unidos, había asistido a la inauguración del primer cable submarino entre Estados Unidos y Europa. En 1849, desde Chile, ya no ocultaba su entusiasmo. Los telégrafos, decía, «aceleran las comunicaciones hasta desaparecer toda idea de distancia», pero se quejaba, también, de que en Argentina no había una voluntad política para invertir en el progreso de las comunicaciones: «Las rutas reales son necesarias, pero también hay que construir las rutas de la palabra».

Las líneas telegráficas existían en Argentina desde 1857, con la presidencia de Bartolomé Mitre, en la época dorada de los ferrocarriles. Las primeras se habían tendido en paralelo a las vías del flamante Ferrocarril Oeste, que unía Plaza Lavalle con Moreno en la provincia de Buenos Aires. Tres años después se inauguraba la primera línea pública de telégrafos de la Argentina, que usaba un equipo Siemens alemán para transmitir mensajes en el código inventado por Samuel Morse[17]: puntos, rayas y espacios, uno tras otro, en un *tracatrá tracatrá* rápido y rítmico de una palanca de hierro contra una madera. Pero mientras que para 1862 el mundo ya tenía 240 000 kilómetros de telégrafos (24 000 en Gran Bretaña, 128 000 en el resto de Europa y 77 000 en América), en Argentina se discutía si había que invertir en la innovación. Finalmente, el avance de la economía y la necesidad de comunicación de la guerra terminaron por imponer la innovación, de la mano de sus grandes promotores: Sarmiento y su ministro del interior Dalmacio Vélez Sarfield.

En esos años de segunda Revolución Industrial y positivismo filosófico, hacer política era hacer progreso, y hacer progreso era hacer ciencia. Los mapas se desmalezaron para imponer los avances del mundo: rutas, puertos, frigoríficos, ferrocarriles y petróleo; y con armas: matando pueblos originarios o mandando a los pobres a morir a la guerra. Las dos eran tareas fundamentales para la idea de progreso

de la Nación en el siglo XIX. En 1864 la provincia de Buenos Aires le concedió a una compañía inglesa la instalación y el uso de un sistema telegráfico para unirla con Montevideo. Se instaló un cable telegráfico subacuático en el Río de la Plata, de 44 kilómetros entre Punta Lara y Colonia del Sacramento, que se completaba con 160 kilómetros que iban por el aire. El resto lo hizo la guerra contra Paraguay, que aceleró el tendido de líneas para comunicar las noticias del combate entre las ciudades de Rosario y Corrientes.

El siguiente salto en las comunicaciones fue la expansión de la red telefónica argentina, que llegó a ser la más importante de América Latina en las primeras décadas del siglo XX. En 1878 comenzaron los ensayos con teléfonos construidos en Buenos Aires, dos años después de la primera comunicación telefónica del mundo (en Boston, Estados Unidos). El «*tracatrá*» del telégrafo era reemplazado por el «*riiing*» de los nuevos aparatos que comenzaron a instalarse en las residencias particulares de los hombres del poder de la época: el entonces ministro del Interior Bernardo de Irigoyen, el presidente de la Nación Julio Argentino Roca y el intendente de Buenos Aires Torcuato de Alvear. Muy pronto, en 1881, ya había un servicio comercial en el país, ofrecido en conjunto con empresas europeas y norteamericanas que proveían inversiones y tecnología. La Unión Telefónica del Río de la Plata, con capitales y administración inglesa, contaba con 6 mil abonados en 1886, y prestó servicios hasta 1929, cuando —ya con 196 mil líneas— fue comprada por la norteamericana International Telephone and Telegraph Company. Desde 1887, la competencia era la Compañía Telefónica Argentina, que en los primeros años del nuevo siglo instaló las primas centrales telefónicas automáticas en varias ciudades claves de la economía argentina: Córdoba, Rosario y Buenos Aires[18]. Cien años antes de la aparición de internet, las compañías de telecomunicaciones ya habían trazado el mapa que luego repetiría el anillo de la actual Red: el triángulo cordobés-rosarino-porteño ya era el más conectado de la Argentina.

Los avances que llegaban de Europa impulsados por la Primera Guerra Mundial y la creciente demanda de los consumidores argentinos, los ciudadanos que se integraban a la Nación luego de las grandes oleadas inmigratorias, dieron en la década del 20 del por entonces nuevo siglo el siguiente gran salto de tecnología y crecimiento de la red. Los procedimientos manuales se automatizaron y se inauguraron centrales en distintos barrios porteños: Barracas, Retiro, Plaza (en Barrio Norte[19]). En 1929, los teléfonos también se conectaron con el mundo: ese año se consiguió el primer enlace internacional entre Argentina y Europa. En 1946, durante el gobierno de Juan Domingo Perón, el Estado cambió su rol de ordenamiento y control de las empresas telefónicas y comenzó a intervenir directamente en la provisión y venta de servicios. Creó la Empresa Mixta Telefónica Argentina, con la que nacionalizó los activos y pasivos de la Unión Telefónica. Diez años más tarde creó Entel (la Empresa Nacional de Telecomunicaciones), que funcionó durante 34 años con capitales estatales y enfrentó los desafíos que supusieron el gran

crecimiento de las comunicaciones internacionales, la llegada de los satélites y luego internet. Los ingenieros que trabajaron en la empresa durante esos años fueron también beneficiarios del Estado: se formaban en escuelas técnicas de prestigio y asistían gratis a las universidades nacionales creadas para formarlos en los oficios tecnológicos, como la Universidad Tecnológica Nacional, inaugurada en 1959, también por impulso de los fuertes sindicatos de la época. Gran parte de esa generación de jóvenes que ingresó al mercado laboral entre los 60 y los 70 fue luego la que se encargó de la instalación de la infraestructura de internet en Argentina. Como sucede ahora con los estudiantes de programación y sistemas, las empresas los contrataban antes de terminar la facultad para instalar equipos y cables en grandes centros de comunicaciones que procesaban una creciente cantidad de conexiones entre la Argentina y el mundo.

Desde 1969, en la esquina porteña de Cangallo (hoy Perón) y Talcahuano, Entel tuvo su Centro de Conmutación Internacional en un edificio de varios pisos, donde se dividían los operadores de las llamadas y los técnicos que manejaban los equipos de transmisión y las mesas de pruebas de las tecnologías que se iban incorporando a las comunicaciones. Veinte años después del primer enlace internacional que se hizo en Argentina, en ese edificio se resolvían todas las llamadas del país hacia el exterior. Pero nada era directo ni fácil ni rápido. Cada conexión se hacía manualmente, previo llamar al triple cero, hablar con una amable operadora (de día; porque la ley todavía no permitía a las mujeres trabajar de noche) y comunicarle el destino de la llamada. Los circuitos internacionales necesitaban chequeos constantes, uno por uno, porque cada conexión se hacía punto a punto y cada canal tenía que estar en condiciones para tomar una llamada tras otra. La demanda era inmensa, sobre todo para España, Italia, Estados Unidos, los países donde los argentinos tenían familiares y las empresas, clientes. La tecnología del momento era el cable coaxial de alta capacidad, inventado en la década del 30 y que gracias a sus distintas capas y conductores de electricidad, permitía realizar simultáneamente más llamadas con mayor velocidad. La compañía estatal también se hizo cargo de las transmisiones por satélite que comenzaron en Argentina también en 1969, el día exacto que el ser humano pisó la Luna. Las transmisiones se operaban con ingenieros en las estaciones terrenas de Balcarce —al sudeste de Buenos Aires— y de Bosque Alegre —cerca de Alta Gracia, en Córdoba —.

También en los 60, comenzaba el siguiente salto tecnológico: el progresivo reemplazo de la era analógica hacia la digital. Los recién inventados microchips iniciaron la carrera por reducir el espacio de los equipos, hasta llegar, en los 80, a la era de la fibra óptica. En 1972, durante la dictadura de Alejandro Lanusse, se sancionó la Ley Nacional de Telecomunicaciones 19 798, que desde entonces y hasta 2014 regularía esa área.

Sin embargo, en medio de esos avances que cambiarían el mapa de las comunicaciones del mundo, el 13 de noviembre de 1990 Entel dejó de ser estatal. En

ese momento, con tres millones y medio de líneas telefónicas fijas, operadas en un 90 % por la compañía, el gobierno de Carlos Menem decidió su privatización. Fue una negociación férreamente dominada por el Poder Ejecutivo, que desestimó quejas de la oposición, intercedió con los sindicatos y aceleró un proceso destinado a obtener la confianza de los capitales extranjeros y los organismos financieros internacionales, mientras se renegociaba la deuda externa. Las privatizaciones, pero sobre todo la de los teléfonos, fueron resueltas vertiginosamente, acompañadas por un optimismo de los medios de comunicación que sostenían que «desprenderse de las empresas públicas significaba acabar con la inflación, la ineficiencia y la baja productividad[20]» y una opinión pública que compartía la idea de la poca eficiencia del servicio, ejemplificada en la demora de más de un año que tardaba la empresa en instalar una línea.

Un año antes, recién iniciado el gobierno de Menem, se había sancionado la Ley de Reforma del Estado. Más conocida como la ley Dromi, por el apellido del ministro de Obras y Servicios Públicos que la había impulsado, la norma sentaba las bases de futura oleada de privatizaciones: autorizaba por decreto no solo el paso a manos privadas de las empresas, sino también la desregulación y desmonopolización de los servicios públicos. Sin embargo, más que una ley desreguladora del mercado, terminó funcionando en favor de una serie de empresas que, amparadas por el Gobierno nacional, crearon un nuevo escenario de monopolios, esta vez en manos privadas.

En el caso de las telecomunicaciones, Telecom y Telefónica, las dos empresas beneficiadas en el proceso, se repartieron las líneas telefónicas del país como el botín de una guerra: el Norte para la primera, el Sur para la segunda, estableciendo un monopolio que dura hasta hoy. Las llamadas internacionales, por su parte, pasaron a depender de una nueva empresa, Telintar, para la que se adquirieron equipos y *routers* nuevos.

—Compramos como locos, durante años, después de las privatizaciones.

Así recuerda esos años Ernesto Curci, el ingeniero que hoy cuida los cables maestros de internet de Level 3 (que salen de Las Toninas) y en los 90, como parte de las telefónicas, se encargó de la instalación previa de la infraestructura de las comunicaciones internacionales que darían nacimiento a internet.

En ese proceso, fueron los mismos ingenieros que antes se encargaban de probar circuitos y perillas en el edificio de Entel de Cangallo, ahora empleados en las telefónicas de capitales españoles[21], quienes se abocaron a la tarea de adaptar la infraestructura para conectarse con el exterior. Primero lo hicieron a través de los cables que ya cruzaban el océano Atlántico hasta Europa para las llamadas internacionales y con algunas conexiones satelitales. Más tarde, entre 1999 y 2001, también fueron los encargados de construir, en Las Toninas, las estaciones de amarre de cables submarinos que luego albergarían los primeros tendidos de fibra óptica.

Pero antes de las privatizaciones argentinas, entre 1987 y 1992, sucedieron en el país y en el mundo una serie de avances fundamentales para el invento futuro:

internet.

En 1984, en el mundo, la computadora personal o PC empezaba a aparecer en las publicidades televisivas, en las revistas y en las cadenas de productos para el hogar como un objeto de deseo para las familias. Los fabricantes, con IBM y Apple a la cabeza, las hacían cada vez más chicas y portables: las sacaban de las universidades e institutos científicos, reducían los espacios que ocupaban en las oficinas y hacían otros modelos, más pequeños, para que cada familia incorporara la computadora como un mueble más, como antes había sucedido con el televisor.

En Argentina, en 1987, las computadoras no eran algo masivo, pero ya había algunos hogares privilegiados que las tenían (como el mío, con mi IBM PS/2) y algunas empresas y universidades comenzaban a usarlas. Fue justamente un grupo de docentes e investigadores de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires el que, en ese año de la primavera alfonsinista, dio uno de los primeros pasos de internet en la Argentina. Con una PC con 10 megas de memoria —menos de la capacidad de un celular actual—, un grupo de pioneros de la carrera de Computador Científico logró enviar los primeros *mails*. En agosto de ese año, el ingeniero Carlos Mendioroz, del mismo equipo, inscribió el registro de dominio superior de argentina, es decir, el .ar. El 23 de septiembre, comenzó a funcionar. Argentina estrenaba su pasaporte en la confederación de países conectados a internet.

Unos años después, algunos de esos integrantes del grupo fueron convocados por la Cancillería argentina para crear una red que la conectara con las embajadas y delegaciones del mundo[22]. «Como quien no quiere la cosa», recuerda el ingeniero Jorge Amodio, protagonista de la historia, realizaron la primera conexión a internet. El 17 de mayo de 1990, a las 19.55, Argentina se convirtió en uno de los primeros países de América Latina en conectarse a la Red. Además de la Cancillería, las primeras conexiones en Argentina las utilizaron las universidades, que fueron creando una serie de redes de intercambio entre ellas y con el exterior[23].

En el mundo, internet había nacido oficialmente un año antes. En 1989, el británico Tim Berners-Lee había establecido la primera comunicación entre un cliente y un servidor y había nacido la web. En 1991 el acceso ya era público en Estados Unidos y desde 1993 ya existían navegadores que traducían los enlaces en hipertextos entendibles por todos. El resto, lo sabemos: portales, *mails*, buscadores, redes sociales, gatitos, selfis, estrellas efímeras de YouTube, odiadores compulsivos de Twitter, comentadores seriales de noticias en portales de información. Pero en los 90 eso recién empezaba y en Argentina, además de los académicos, también se sumaban emprendedores que se las ingeniaban para comprar enlaces y armar sus redes[24].

Sin embargo, todavía debían suceder una serie de conflictos entre el Estado argentino, las empresas proveedoras de servicios y los nuevos jugadores que buscaban insertarse en el nuevo mercado de internet.

En 1990, el pliego de privatización de Entel le había otorgado siete años de exclusividad a las empresas prestadoras de servicios, Telecom y Telefónica, con la posibilidad de extensión por tres años más, si cumplían con las inversiones requeridas en el acuerdo. La telefonía fija había quedado en manos de las dos empresas. Pero otros servicios, como los satelitales de datos, en los primeros años de internet en Argentina, estaban fuera de toda regulación y podía ofrecerlos cualquier empresa. No obstante, el gran obstáculo era que todos los enlaces internacionales había que comprarlos a la empresa que se había quedado con las comunicaciones internacionales, Telintar. Y esa empresa, durante años no habilitaba enlaces, y si lo hacía, ponía unos precios exorbitantes. Algunas universidades y grupos de investigadores reclamaron el acceso a esos enlaces, en un momento en que conectarse a la Red ya era un requerimiento profesional indispensable para comunicarse con otras universidades y centros de investigación.

Por ese motivo, internet no fue masiva hasta 1995, cuando se creó Startel, el primer proveedor de internet del país, una empresa que contaba con participación Telecom y Telefónica en partes iguales. Ese año se inició la Red comercial, que usaba la red telefónica para conectarse e introducía un nuevo sonido característico a las comunicaciones. El sonido que abría la puerta al mundo para navegar en una Red que entonces ya tenía 30 millones de usuarios en el mundo. Junto con Colombia, Argentina fue el país latinoamericano en el que más crecieron los accesos a internet. Pero los precios todavía eran muy altos y se cobraran por minuto.

En 1997, cumplidos los siete años de exclusividad que habían fijado las privatizaciones para Telefónica y Telecom, el gobierno de Carlos Menem extendió el acuerdo por tres años más, aun cuando las empresas no habían cumplido con las inversiones[25]. Las dos empresas seguían siendo las principales operadoras del nuevo mercado de internet, hasta que, en 1999, con el nuevo gobierno de Fernando de la Rúa, se inició una apertura del mercado hacia nuevas empresas, buscando atraer inversiones.

—Desde la Comisión Nacional de Comunicaciones hicimos una campaña avisando a las empresas que podían venir a invertir —recuerda Henoch Aguiar, especialista en telecomunicaciones y parte de la comitiva del gobierno de la Alianza que viajó a Washington y Londres a vender esa apertura a las empresas de telecomunicaciones del mundo.

Quince años después, Aguiar, un hombre de énfasis, en palabras y gestos, lapicera en mano, defiende su decreto 764 de 2000, que permitió a las empresas de comunicaciones ampliar el mercado y construir lo que hoy sigue siendo la base de internet: los cables submarinos de fibra óptica y la posterior red que unió en anillos a todo el país.

—Necesitábamos la mayor cantidad de competencia posible. Esa apertura hizo que vinieran seis mil millones de dólares en los peores años de la Argentina.

A partir del decreto del 9 de noviembre de 2000 llegaron inversiones de Impsat (Grupo Pescarmona), Techtel (Tecnhint y Telmex), Keytech (AT&T), Global Crossing (luego comprada por Level 3) y las mismas Telefónica y Telecom, que se sumaron a la carrera para no quedarse detrás.

Entre 1999 y 2001, se produjo la mayor expansión en caños, tubos y cables de internet de la ciudad de Buenos Aires y del país. Fueron seis mil millones de dólares invertidos en redes de internet en tres años, mientras el país atravesaba una de las peores crisis socioeconómicas de su historia, que había terminado con un 22 % de desocupación y 39 argentinos muertos por policía en las protestas callejeras del 19 y 20 de diciembre de 2001. En ese país que estallaba y se veía en las portadas de los entonces nuevos medios *online*, crecía la infraestructura de la nueva tecnología de masas. La imagen del «progreso» le ganaba a la crisis. O se le imponía. En Las Toninas, las empresas de telecomunicaciones contrataban la experiencia de multinacionales como Alcatel y Tyco, que ya instalaban redes en el mundo y empleaban a operarios e ingenieros locales en un frenesí por construir contra reloj. En el preciso momento de la apertura del mercado, en noviembre del año 2000, querían tener sus estaciones de amarre de fibra óptica listas para empezar a operar los cuarenta mil kilómetros de cables instalados. Esa bestia submarina de luz y cable es la que todavía hoy usamos y por la que hoy van y vienen nuestros datos.

En los siguientes quince años, la Red creció según las necesidades del mercado. El 70 % de los argentinos, concentrados solo en el 30 por ciento del territorio, tienen una buena conexión, que no está por sobre los estándares regionales. Pero el restante 30 por ciento que ocupa la mayor extensión del territorio tiene una conexión de muy baja calidad.

Hoy, muchas ciudades pequeñas tienen una conexión 10 o 20 veces peor que las grandes áreas urbanas. La red de Telecom tiene 21 650 kilómetros y la de Telefónica 25 000 kilómetros[26], pero todavía existen partes del territorio de Argentina que se encuentran subconectadas. Esto llevó a que, desde 2011, el Estado argentino se sume a la expansión de la infraestructura a través del programa Argentina Conectada[27], con el objetivo de tender redes complementarias a las de las empresas privadas allí donde, por razones de inversión económica, las tres compañías que dominan el mercado no llegan. Hasta ahora, se construyeron 15 453 kilómetros de la red y 4494 kilómetros se compraron de otras empresas. Adicionalmente, se firmaron acuerdos con Telecom y Telefónica para acceder a 8305 kilómetros de sus redes. Eso suma 28 252 kilómetros, de los 58 000 que espera instalar el proyecto. El objetivo del plan, además de llegar a lugares sin conexión (y a escuelas, bibliotecas y dependencias públicas) es que el Estado se convierta en otro proveedor de internet y sumar otro jugador que baje los precios. El plan hasta ahora avanzó en estos resultados. En la provincia de Tierra del Fuego, instaló 100 kilómetros de fibra óptica para cruzar desde el continente por el Estrecho de Magallanes y resolver un déficit histórico de conexión de los habitantes y las empresas de tecnología de la isla, que antes se

conectaba solo mediante radioenlace, una tecnología cara y susceptible de funcionar mal por razones climáticas.

Junto con esta intención de intervención estatal en las comunicaciones digitales, el 29 de octubre de 2014, el gobierno de Cristina Fernández de Kirchner, presentó el proyecto de ley Argentina Digital, para reemplazar y modernizar la Ley de Telecomunicaciones de 1972. El anuncio fue sorpresivo pero necesario, ya que la antigua legislación había quedado no solo vieja, sino antigua, luego de los cambios en las tecnologías. En 2014, pero desde décadas anteriores, ya se había iniciado el llamado proceso de convergencia, es decir, la capacidad de proveer distintos servicios a través de una misma infraestructura: voz, audio, video y datos en general. Si en los 60 se necesitaba «un cable» para ofrecerlos por separado, cincuenta años después los avances permitían hacerlo con el mismo.

—Vamos a tener redes que le faciliten a la gente acceder al mayor universo de información posible dentro de lo que técnicamente los argentinos estamos en condiciones de ofrecer —dijo el ministro de Planificación Federal, Julio de Vido, la mañana de la presentación del proyecto de ley en el microcine del Ministerio de Economía.

De Vido defendía el flamante proyecto en el contexto de otras iniciativas que había desarrollado el Estado nacional en los últimos años con el objetivo de reposicionar a la Argentina en su soberanía de comunicaciones. Entre ellas se encontraba el Arsat-1, el primer satélite geoestacionario construido en el país, que se había lanzado ese mismo mes de octubre, con una gran repercusión en los medios. Para el Gobierno, la puesta en órbita del Arsat era parte de un plan de infraestructura digital que también incluía el tendido de redes de fibra óptica de Argentina Conectada y ahora una nueva ley, que iba a modificar también la competencia en el mercado. Por eso, la misma mañana en que se presentaba Argentina Digital, el ministro de hacienda Axel Kicillof, lo defendía:

—Por un lado están las redes, el transporte, el cable que te llega a tu casa. Esa es una cuestión. Y separado de eso están los contenidos. Este proyecto pone como servicio público la infraestructura que permite que lleguen a tu casa los datos. Todo es digital, no analógico. Lo que llega adentro del cable, el contenido, es libre. Esta ley no regula contenidos.

El proyecto presentado proponía regular y abrir el mercado de «los caños», pero prometía no inmiscuirse en lo que sucediera con los contenidos. Al mismo tiempo, permitía a otras empresas (no solo a las telefónicas, sino también a las audiovisuales) brindar servicios de telecomunicaciones, en especial los de Triple Play (la provisión de servicios de datos y voz por parte del mismo proveedor). Con esto, la ley proponía adaptar a la Argentina al cambio tecnológico y convertir a su futura autoridad de aplicación también en una reguladora de las ulteriores inversiones, velocidades de conexión y acuerdos de interconexión de las redes. El objetivo era dar una mayor intervención del Estado en un mercado concentrado, donde los usuarios siempre

quedaban atados a las decisiones corporativas en un servicio tan básico como las telecomunicaciones. Otro punto importante de Argentina Digital era que, por primera vez en una legislación nacional, se dejaba por escrito el concepto de neutralidad de las redes, es decir, la imposibilidad de que los prestadores de internet manejaran el tráfico con discrecionalidad (por ejemplo, dándole menor velocidad a servicios para ver películas o a redes sociales de uso masivo, para evitar la saturación de sus «caños»). Y además fijaba la inviolabilidad de las comunicaciones, una medida relevante, en tanto garantizaba que ningún proveedor, organismo público o privado podía atentar contra lo que los ciudadanos escribieran o compartieran en su uso diario de internet. En la letra, el proyecto era casi «idealista» en muchos aspectos con los que la legislación de telecomunicaciones no se había inmiscuido en décadas. Tal vez también por eso los especialistas recomendaron cautela: los monopolios telefónicos, audiovisuales, tecnológicos y de contenidos seguramente se enfrentarán en los próximos años con un Estado dispuesto (al menos en su discurso inicial) a interceder en sus poderes, concentrando él también una gran potestad de decisión en manos de la nueva autoridad de aplicación de la ley.

Luego de intensos debates en las comisiones de comunicaciones de la Cámara de Diputados y Senadores, la ley Argentina Digital fue aprobada, el 16 de diciembre de 2014. Para algunos legisladores opositores, organismos de derechos de internet y académicos, la sanción fue apresurada. Entre las críticas, se señala que la autoridad de aplicación, es decir, el órgano encargado de implementar la norma a futuro, cuenta con atribuciones excesivas y pocos mecanismos de control. También hubo disconformidad en algunas empresas telefónicas, que se quejaron de que la ley no estaba hecha para facilitar las inversiones por la gran injerencia estatal. Sin embargo, desde la Secretaria de Comunicaciones, Argentina Digital fue defendida para intervenir en el mercado y para garantizar que los distintos proveedores (telefónicas, empresas de cable o de internet) interconecten sus redes con arquitecturas más abiertas, desagregando las estructuras locales. Es decir, el objetivo —en lo escrito— es romper, o al menos debilitar, el monopolio actual de las comunicaciones digitales.

Hay un punto en el que oficialistas, opositores y académicos coinciden: el sendero estará plagado de obstáculos.

Finalmente, en la Argentina y en el mundo las tecnologías siempre avanzan, o se imponen, por necesidades de los usuarios o (más frecuentemente) del mercado. Las leyes pueden impulsarlas, reprimirlas o modificar su adaptación para dar más o menos ganancias a las empresas, pero el camino es hacia adelante. Por las guerras que aceleran los inventos, por el mercado y su necesidad de vender lo nuevo a la mayor cantidad de consumidores posible, o por la inevitable necesidad del ser humano de comunicar sus noticias (corriendo de un pueblo a otro, en los inicios de la civilización; reduciendo distancias con inventos, más tarde). Pero también por la seducción esperanzadora de todo «progreso». Esa que hoy nos sigue cautivando cuando la vemos avanzar en la ciudad, con una capa que tapa a otra, tal vez todas

ellas invisibles mientras caminamos, conectados a la radio, a los *mails*, a los mensajes para encontrarnos con alguien en la otra esquina.

III

Los dueños de internet, más allá de Mark Zuckerberg

> «A veces ciudades diferentes se suceden sobre el mismo suelo y bajo el mismo nombre, y mueren sin haberse conocido».
>
> ITALO CALVINO.
> *Las ciudades invisibles* (1972).

Ráfagas de perfume francés, mezclado con caramelos de mentol y naftalina, impregnan el corredor del Teatro Colón para el abono vespertino. El programa de la tarde es un homenaje por los 150 años del nacimiento de Richard Strauss. Por unas horas, en un lugar de la ciudad nadie agacha la cabeza para chequear el celular. En este edificio de 1908, la única señal de modernidad son los auriculares verdes con luces de un pelirrojo que escala hacia la tertulia silbando la *Marcha Imperial* de *Star Wars*. En minutos, las luces se apagan y el público deja la sala en silencio para recibir a la Filarmónica de Buenos Aires.

Cruzando la calle, sobre la vereda de Cerrito, se despliega otro espectáculo. Esta vez, en lugar de músicos en frac, la orquesta está compuesta por una cuadrilla de obreros con uniformes azules de tela gruesa y botas embarradas hasta la rodilla. Sus instrumentos son chalecos cargados de pinzas y taladros que rompen la vereda. Levantan las baldosas y cavan sesenta centímetros tierra hacia abajo. Allí, el conjunto de cirujanos-operarios encuentra capas de tierra pedregosa y tubos de todo tipo de tamaños y colores. Son las arterias que dan comodidad a sus habitantes: gas, agua, electricidad, teléfono, internet. Antes de que termine la noche, tienen un objetivo: empalmar tres capas de tubos con una conexión de internet que viene, por debajo de esa vereda, desde la calle Lavalle. Están expandiendo una red para llegar con un nuevo cable a una empresa que necesita más capacidad para una gran base de datos. Es un trabajo de rutina.

El capataz les da un descanso. Los hombres están removiendo capas de ciudad desde las cuatro de la tarde y ya está oscureciendo. Uno de ellos vuelve del kiosco con dos botellas de Coca-Cola y se decretan diez minutos para aflojar los músculos. Mientras unos se apoyan en las vallas y otros estiran los brazos sobre el camión de herramientas, escuchan una voz de mujer acercándose hacia ellos.

—¿Quién les dio permiso para romper esta vereda?

La señora sale de su edificio, a metros del Obelisco porteño, con un manojo de llaves pesado en la mano y busca con la mirada al portero para increpar a los obreros.

—¿No ven que estamos a una cuadra del Colón? Es una zona de categoría, no puede levantar la vereda de esta forma.

—Buenas tardes, señora. El encargado de su edificio puede facilitarle el permiso de obra del Gobierno de la Ciudad de Buenos Aires. Quédese tranquila que para las nueve, diez de la noche, nos retiramos.

—Se la pasan arruinando la ciudad —se queja la mujer, volviendo tras sus pasos para buscar el permiso que le acerca el encargado—. ¿Por lo menos me puede decir de qué es la obra?

—De internet.

Pablo Aguirre Paz responde rápido y vuelve a supervisar la zanja de cincuenta centímetros de ancho y casi media cuadra de largo que su cuadrilla está llenando con tubos. Aprendió a calmar vecinos en los 15 años que lleva trabajando en Iplan, una empresa de provisión de internet y centros de datos para empresas. Pablo ingresó en la compañía a poco de fundada, con pocas materias para recibirse de ingeniero civil en la Universidad Tecnológica Nacional, en plena etapa de construcción de una red que hoy —solo en su empresa— cubre 320 manzanas de Buenos Aires con 160 kilómetros de instalaciones y otros 100 kilómetros en otras ciudades del país. Maratonista, flaco de cuello largo y chomba rayada, Pablo puede enumerar sin errores, sobre un mapa de la ciudad, por dónde pasa cada caño, sube cada cable y se conecta cada tramo de fibra óptica. Cuando empezó, en el año 2000 —mientras Argentina iniciaba el descenso a una de las peores crisis de su historia—, su empresa construía a un ritmo de diez obras por día y él era uno de los dos supervisores que se encargaban de pedir los permisos, coordinar las cuadrillas, vallar las veredas, las calles o las estaciones de tren, y avanzar. Fueron años sin descanso. Pero no solo para sus hombres, sino para el resto de las empresas.

La internet que hoy usamos se construyó en esos años. Su esqueleto sigue creciendo en kilómetros. Las tecnologías avanzaron, pero algo no cambió: quince años después, el orden del mercado se sigue imponiendo en la ciudad. Donde se necesiten cables o tubos más grandes para llevar una internet más potente, allí se instalan. No importa lo que suceda debajo de la vereda o arriba, en los edificios. No importa cuán caros sean los mármoles de entrada o el bronce de las puertas. La tarea de las empresas que construyen y hacen funcionar internet no descansa. Su reino está debajo de la tierra, en huecos oscuros o espacios donde pocos llegan, como los montantes o las terrazas de los edificios, donde sus cables se encuentran con otros hilos del progreso y funcionan a pesar de su aspecto de madejas desordenadas.

Cómo nos conectamos a internet, cuánto la pagamos, a qué velocidad navegamos y cómo funciona dependen, en gran parte, de las decisiones de una serie de empresas. La Red tiene «dueños» en los distintos niveles que se necesitan para que funcione: la infraestructura (los «caños», el esqueleto de la bestia), los estándares (su idioma: las

reglas y los protocolos que sigue la información para llegar a destino) y los recursos que intermedian entre los aparatos y las personas (cómo piensa: el *software*, los programas).

En la jerga técnica este es el «nivel de la infraestructura». Y es vital. Pero lo damos por sentado, como el oxígeno cuando respiramos o la electricidad cuando encendemos la televisión. También nos olvidamos de que esos caños tienen dueños. Para las empresas que los manejan eso es bueno: si no sabemos quiénes son, no podremos reclamarles cuando la conexión se cae o cuando pagamos mucho por una velocidad deficiente. También lo estimulan cuando nos presentan la idea de la nube, de los jóvenes en los parques siempre conectados, con chats que se abren como globos de colores colgados de la nada, contra un fondo soleado y feliz.

Internet es la estructura artificial más grande y compleja creada por la humanidad. Es también, nuestra creación más colectiva: la que más partes necesita, al mismo tiempo, tomando decisiones conjuntas. Pero sus dueños materiales no son tantos y pueden dividirse en dos grandes grupos: los proveedores de tránsito y los proveedores de contenidos. Entre ambos se divide el reino de internet. Y también, entre cada bando, se está librando la primera de las guerras de internet: la batalla por la neutralidad. La base de esta lucha es económica: quién paga la inversión en «caños» que requiere un uso cada vez más intensivo de la Red. ¿Los proveedores de internet, es decir, los que construyeron el monstruo de internet? ¿O las empresas de contenidos, aquellas que más usan los cables y hoy ganan más dinero en internet? ¿O ambas? Para comprender la guerra, hay que sumergirse una vez más en las entrañas del animal.

Los proveedores de tránsito son las empresas que nos proveen de la «ferretería[28]» para comunicarnos: tubos, cables, fibra óptica, *routers*, centros de datos. En la Argentina, y también en el mundo, muchos de estos proveedores (también llamados ISP[29]) son las compañías telefónicas que ya contaban con instalaciones de telecomunicaciones y un conocimiento técnico previo a la llegada de internet, y con la llegada de las nuevas tecnologías de información y comunicación sumaron un nuevo servicio (y negocio). En el caso argentino, estas empresas son Telefónica y Telecom, que se quedaron con el servicio telefónico luego de las privatizaciones de la década del 90. También son proveedores de tránsito empresas de televisión por cable, como Fibertel (del grupo Clarín-Cablevisión) en Argentina, o Comcast en Estados Unidos. Fuera de los grandes centros urbanos, existen también cooperativas telefónicas o eléctricas locales, pequeñas empresas de cable o pymes de pueblos y ciudades que también ofrecen servicios de internet, a menor escala.

Los proveedores de tránsito brindan el servicio de conexión que usamos todos los días para comunicarnos. Son los contratistas de la «autopista» de los datos[30]. Instalan y reparan la infraestructura en nuestras casas, pero también se encargan de

montar y mantenerla afuera: en sótanos, terrazas, debajo de la vereda o en caños que viajan al lado de las vías del subte para cubrir muchos kilómetros sin ser interrumpidos. Para hacerlo, estas empresas manejan ejércitos de ingenieros y operarios que recorren la ciudad con palas, mapas y permisos municipales. Gran parte del trabajo diario de estas empresas es negociar las «servidumbres de paso» con los gobiernos municipales, provinciales y nacionales, es decir, los lugares por donde pasarán los cables para seguir expandiendo su infraestructura, para sumar conexiones o para reparar las existentes.

Además del nivel local, hay otro eslabón del tránsito que se encarga de enchufarnos al mundo, es decir, de integrar la infraestructura local con la internacional. Estas empresas —también concentradas, con Level 3 y AT&T a la cabeza— proveen lo que en la jerga se llama el *backbone*, es decir, la columna vertebral, las enormes instalaciones de caños terrestres y submarinos que cruzan continentes, países y océanos para que internet pueda ser una Red global. A esa columna se acoplan luego las vértebras locales, los *backbones* que están en nuestro territorio. En Argentina, sus dueños son también Telecom y Telefónica, que alquilan a las empresas internacionales algunos tramos para pasar sus propios cables. A su vez, las empresas más chicas, por ejemplo las cooperativas eléctricas de pueblos a los que no llegan las grandes compañías de internet, también alquilan «caños» a las telefónicas más grandes. Esto hace que, aunque la Red se componga de un despliegue horizontal de infraestructura en millones de rincones muy dispersos, su estructura esté integrada verticalmente. Internet es una serie de redes que transportan redes: desde las más grandes a las más pequeñas.

Si los proveedores de tránsito locales son pocos y concentrados, los de las comunicaciones internacionales lo son aún más. Y, como son los dueños de los caños que cruzan países y continentes, todo el planeta les paga a ellos para comunicarse. Entre estas empresas la más importante es Level 3, que se encarga de resolver las necesidades del 72 % del mercado mundial. En términos concretos: 72 de cada 100 palabras que intercambia cualquier ser humano de la Tierra vía internet pasan por su infraestructura. La compañía, con sede en Bloomfield, Colorado, Estados Unidos, tiene una gran presencia en América Latina, especialmente en Argentina, Brasil, Chile, Colombia, Ecuador, Perú y Panamá, por donde circulan sus redes, construidas en forma de anillo de fibra óptica. Junto con ella, las otras empresas que se encargan de la mayor parte del tráfico internacional son Cogent Communications, Tinet (ambas con sede en Estados Unidos) y Telia Sonera (Estocolmo, Suecia), entre otras[31].

Las sedes físicas de estas corporaciones también nos muestran que nuestros datos viajan por rutas cuyos dueños generalmente desconocemos, pero construyen los caminos y nos cobran por usarlos. También nos revelan que un grupo de empresas que se pueden contar con los dedos de la mano resuelven los caminos de internet de 2400 millones de usuarios en casi 200 países. Sin embargo, al contrario de lo que sucede con las caras, biografías y riqueza de otros protagonistas de internet, como

Bill Gates de Microsoft o Mark Zuckerberg de Facebook, conocemos muy poco sobre estas empresas que también controlan gran parte de los datos que confiamos a la Red[32]. Gates, fundador y dueño de la empresa de *software* más usada en el mundo, Microsoft. Zuckerberg, dueño de Facebook, la red social que conecta al 40 % de los usuarios de internet del mundo. Con ellos, Larry Page y Sergei Brin, propietarios de Google, conforman el otro grupo de amos de internet: los proveedores de contenido. Son quienes controlan las empresas por donde pasan nuestros datos, que también necesitan de una gran cantidad de infraestructura para funcionar. Son los que inventaron y mantienen las otras estructuras por las que pasan nuestras vidas conectadas: los programas de la computadora (si usamos Windows, el dueño es Bill Gates; si tenemos Mac y usamos su OS es Tim Cook, que reemplazó a Steve Jobs tras su muerte), el celular o la tableta (si usan Android, la dueña es Google, si usan Windows Mobile, un iPhone o un iPad, vuelven a ser Gates o Cook), las aplicaciones con las que gestionamos nuestra vida, las redes sociales por donde nos comunicamos (Zuckerberg por Facebook e Instagram, Jack Dorsey por Twitter), las plataformas en las que vemos películas (Reed Hastings si usan Netflix); y los términos y condiciones que las regulan.

De este grupo, los dueños de los contenidos, sabemos bastante más. Eso no quiere decir que sus vidas escapen a las manipulaciones del *marketing* o la prensa, pero relacionamos sus nombres con sus empresas, alguna vez les vimos la cara en una nota y todos ellos aparecieron en algún capítulo de *Los Simpsons*. Forman un grupo de celebridades de la tecnología, aunque, en su interior, es un grupo heterogéneo. Sus edades van desde los 58 años de Bill Gates a los 30 de Mark Zuckerberg, pasando por los cuarentones Larry Page de Google o Jack Dorsey de Twitter. Casi todos (menos Steve Jobs, autodidacta a la fuerza, porque no podía pagarse la universidad) tuvieron una educación de elite: Harvard, Yale, recibidos con honores en ciencias de la computación en sus universidades locales y luego doctorados en Stanford. Sus familias también hablan de ellos: el ruso Sergei Brin, cofundador de Twitter, es hijo de una investigadora de la NASA y de un profesor de matemáticas y está casado con una de las biotecnólogas más reconocidas de Estados Unidos, egresada de Yale. Larry Page, uno de los fundadores de Google, casado con una experta en biomedicina, es hijo de una profesora de programación de la Universidad de Michigan y su padre, también experto en código, fue pionero y autoridad en los desarrollos de inteligencia artificial. Pero en otros casos se criaron con un padre dentista y una madre psicóloga, como Mark Zuckerberg, o de un empleado ferroviario y un ama de casa, como Steve Jobs. Tampoco tienen en la religión una coincidencia, y van desde los agnósticos como Bill Gates, a los budistas como Steve Jobs o los judíos, practicantes y no tanto, como Zuckerberg y Sergei Brin. Políticamente sí se encuentran en su mayor afinidad con el Partido Demócrata de los Estados Unidos, que también cosecha más adeptos en el estado de California, sede de Silicon Valley, donde estas empresas se nuclean.

Reed Hastings, el presidente de Netflix, es un miembro activo del partido y Bill Gates declaró públicamente su apoyo a Barack Obama en las elecciones de 2008[33].

Pero de los dueños de las empresas proveedoras de tránsito sabemos casi nada, lo que nos confirma su paso invisible por nuestras vidas. En este grupo sí hay afinidades: sureños, protestantes, ingenieros que combinaron lo técnico con las finanzas, y tan cercanos al Partido Republicano como a la corporación militar de Estados Unidos. También comparten un pasado en una industria mucho más dura, pragmática y alejada de los *flashes*: la de las telecomunicaciones —*telcos*, en la jerga —, donde se formaron, durante la época de las grandes redes telefónicas. Son hijos del *baby-boom* posterior a la Segunda Guerra Mundial, la generación de niños que vio llegar a Neil Armstrong a la Luna y escuchó los acordes de algo nuevo llamado *rock* en su adolescencia. Son una generación de ingenieros que ya sabían de redes de comunicaciones antes de internet, que conocían la tradición tecnológica de conectar el mundo a través de cables. También fueron tejiendo vínculos con el Departamento de Defensa de los Estados Unidos, que, junto con la Universidad de California, desarrolló Arpanet, la primera red experimental de computadoras que daría origen a internet, en 1969. Los científicos de computación e ingenieros que avanzaron en los inicios de internet lo hacían al mismo tiempo que la Rand Corporation de Los Ángeles[34] investigaba, a pedido de la Fuerza Aérea norteamericana, cómo diseñar una red de comunicación capaz de sobrevivir un ataque nuclear.

¿Quién es Jeff Storey, el CEO de Level 3, la propietaria de la mayor cantidad de caños de internet del planeta? Egresado de ingeniería en Telecomunicaciones de la Universidad Metodista del Sur de Dallas, Texas, expresidente de varias empresas de comunicaciones en Oklahoma, 53 años, residente del estado de Colorado, según *Forbes* ganó 8 millones de dólares en 2013, el año en que se hizo cargo de la compañía. Randall Stephenson, el hombre al mando de AT&T, tiene 54 años, nació y estudió finanzas en Oklahoma, fue propuesto por el expresidente republicano George Bush para presidir el Comité Nacional de Seguridad de Telecomunicaciones y es un miembro activo del directorio de la Asociación de Boy Scouts de Estados Unidos. Lowell McAdam, el CEO de Verizon Communications, otra de las empresas de telecomunicaciones más poderosas del mundo, también ingeniero y con master en finanzas, comenzó su carrera en la Marina de Estados Unidos y luego estuvo al mando de grandes compañías de comunicaciones como Bell.

La Red tiene, desde su origen, un fuerte vínculo con la corporación militar, al que luego se sumaron las compañías de telecomunicaciones en su expansión física, hacia la década de los 80. No casualmente, los expresidentes de las *telcos* luego se convirtieron líderes de las empresas de internet, también aprovechando la privatización de muchas empresas telefónicas estatales a fines de los 80 y principios de los 90. Tampoco asombra que esta corporación de ingenieros-empresarios-propietarios de internet haya ocupado, y se haya intercambiado entre sí, los lugares de poder, primero en las *telcos* tradicionales, luego en las empresas de tecnología

proveedoras de internet, pero también en las agencias estatales vinculadas con la seguridad y el monitoreo informático como la Agencia Nacional de Seguridad (NSA), en los últimos años más conocida por las revelaciones de espionaje masivo de Edward Snowden[35]. Ese es su origen y esas son las relaciones en su interior.

Los dueños de los proveedores de contenidos —Zuckerberg, etc.— llegaron después, cuando la Red dejó de conectar solamente universidades y agencias estatales y fue llegando a la gente, a los usuarios comunes, con la expansión masiva de la Red a principios de los 90. En esa década comenzaron a crecer las compañías de Silicon Valley, el grupo de propietarios cuyo poder reside en una combinación de conocimientos técnicos y el espíritu emprendedor. «Los Zuckerberg» nacieron cuando ya existía internet en el mundo, se sumaron a un invento en el que ya venían trabajando otros humanos-ingenieros-empresarios-militares. Los dueños del esqueleto, de los caños y la infraestructura venían «desde afuera» de la Red, de otras industrias. Los creadores de las empresas de contenidos ya crearon sus innovaciones desde dentro de ella.

Para la próxima generación —la que hoy está en la escuela primaria transitando la última época de coexistencia entre los libros y las tabletas— ya no habrá ni adentro ni afuera: internet ya es una, somos incapaces de determinar sus fronteras; nos rodea y trasciende. Mientras tanto, entre los dos grupos, los dueños del tránsito y lo dueños del contenido, la guerra ya comenzó.

En su oficina de Buenos Aires, Pablo Aguirre Paz todavía guarda algunos mapas en papel del recorrido de los cables de internet, aunque desde hace algunos años los mapas ya están digitalizados, en su computadora o en las de la empresa. Sobre un plano de la ciudad, unas líneas de microfibra pintadas a mano marcan el recorrido de las instalaciones. En rojo, las líneas más extensas de la red, muestran los tubos que se extienden durante cuadras, en línea recta, rodeando las manzanas. Desde esas mismas líneas se desprenden otras, pequeñas, que «suben» en el número de casa o edificio preciso de manzana donde la empresa tiene un *hub*, es decir, un dispositivo que centraliza el cableado de una red para poder ampliarla. En general, son «cajas» de color arena, donde se recibe una señal y luego se emite a diferentes puertos o clientes, que somos nosotros.

En el caso de las empresas telefónicas que brindan internet, los *hubs* también se pueden ver en toda la ciudad en forma de unos tótems rectangulares, de un metro treinta, siempre pegoteados con carteles de bandas de *rock*, clases de inglés, paseadores de perros o papelitos de oferta de explotación sexual. Nuestros datos, los del vecino y los de nuestros hijos están dentro de esas cajas cubiertas de erotismo publicitado. Casi extinguidos los teléfonos públicos de la ciudad, las marquesinas donde antes se pegaban los papelitos de las fantasías, los *hubs* de internet hoy se convirtieron en los exhibidores de la industria del sexo. Tal vez no sea un lugar

casual, ya que la pornografía, la forma privada del sexo y la otra manera de explotación de los cuerpos, constituye el 30 por ciento del tráfico de la Red. Fuera de su involuntario papel de clasificados sexuales, cada una de esas cajas tiene varios cables, en general de cobre (en el caso de las telefónicas o empresas de cable que brindan internet), y otros aparatos que multiplican la potencia de la señal y que se fueron agregando con los años para abastecer la creciente demanda de ancho de banda. Algunas también tienen fibra óptica, todavía no tan extendida, pero ya en crecimiento y como próxima renovación masiva de la infraestructura del futuro cercano.

En el mapa de dos metros, desplegado sobre el escritorio de Pablo en su oficina de Montserrat, también hay unas líneas azules. Son conexiones que completan las troncales (las rojas) y que suelen unir dos puntos de la red para pedidos más puntuales de un cliente. En el plano de esta búsqueda del tesoro de internet las líneas azules cruzan, por ejemplo, la Avenida 9 de Julio, la calle Tucumán, para dar conexión al subte o a un cliente que tiene un local subterráneo.

Además de los tendidos de tubos con cables y los *hubs* donde distribuyen las conexiones a cada cliente, los proveedores de internet completan su mapa de acción con los NOC**[36]** o centros de operaciones de Red. Cada empresa tiene uno o varios NOC desplegados en distintos puntos de la ciudad, que pueden ir desde una habitación o un piso de un edificio cualquiera hasta un lugar específicamente destinado a esa función. Los NOC más grandes tienen más equipos de monitoreo de la Red y en algunos casos también albergan servidores, es decir, equipos de almacenamiento de datos. En esos casos, el NOC convive con un *datacenter* o centro de datos. La función de estos espacios donde vive internet es controlar y monitorear las redes con diferentes tecnologías, por ejemplo, las transmisiones de redes de internet y celulares o de distintos tipos de conexiones de internet. También sirven para proveer de «redundancia» geográfica, esto es, que una misma red tenga presencia en varios puntos de una ciudad, a través de la multiplicación de las señales. Finalmente, otra de sus funciones más importantes es la seguridad: en los NOC se controla, segundo a segundo, la provisión de energía y cualquier fallo de la red, que puede ir desde un corte de electricidad a una tormenta, o el corte de un cable o un tramo de fibra por una obra en la calle. Dentro de ellos también vive una parte del monstruo de internet, cuidado por un ejército de hombres rudos, técnicos, formados en la precisión, pero que tratan a los cables y a sus casas como parte de sus familias.

—Cuando mi abuela me pregunta dónde trabajo yo le digo que en un lugar como los nichos de los cementerios, pero sin los muertos.

Leandro Fariña mira las pilas de servidores, uno sobre otro, como cajas de zapatos iluminadas, se asegura que todas las luces estén encendidas y cierra una de las puertas herméticas del *datacenter*. Su reino es este: un edificio en el Distrito Tecnológico de Buenos Aires, en Parque Patricios. El centro de datos, inaugurado en 2012, es el más moderno de la ciudad de Buenos Aires, pero sus dueños, la empresa

Iplan, lo bautizaron «Ringo», el apodo del boxeador Oscar Natalio Bonavena, un peso pesado nacido en el barrio, como un contraste de tradición a su modernidad. Desde la calle, la construcción pasa desapercibida. Sus paneles negros y el cemento gris la camuflan entre los árboles. Pero con solo cruzar el portón de aluminio, los cinco guardias de seguridad que revisan a cada visitante demuestran lo contrario: lo que pasa aquí sí es importante.

Mirando el mapa de internet desplegado en la ciudad, los centros de datos (o *datacenters*) aparecen como conectores ubicados en el extremo de los tubos que nos conectan. Son necesarios para almacenar y distribuir los datos que circulan por los cables (debajo de la tierra, en la terraza de un edificio, en el cable que entra en una laptop). Están distribuidos en la ciudad[37], como parte del sistema nervioso de internet. En estos nodos, los datos, como neuronas, llegan, se acumulan, se comunican con otras que están lejos y se cargan de energía para seguir transmitiendo o haciendo sinapsis con otra información. A medida que la información crece, los *datacenters* también necesitan expandirse. Antes, nuestros datos (*mails*, tuits, películas, posteos de blogs, comentarios en diarios *online*, episodios de la serie *Mad Men*, búsquedas de vacaciones en Google) cabían en habitaciones pequeñas, en un par de armarios, pero hoy los *datacenters* ya son varios edificios en cada ciudad y sus suburbios: cuanta más gente y más conectada, también crece la densidad del espacio de almacenamiento.

Los libros que ya no ocupan bibliotecas de madera porque los bajamos en el Kindle, la docena de facturas de teléfono anuales que ya no acumulamos en un cajón porque las pagamos *online*, los DVD que no se apilan más en la mesa del televisor porque están en Netflix, los álbumes de fotos que dejan de juntar tierra en un placard reemplazados por Instagram: todo eso salió de nuestras casas y ahora tiene un nuevo hogar, llamado *datacenter*.

Además de gestionar los 144 mil millones de correos electrónicos diarios que circulan en el mundo[38], en los *datacenters* también se acumulan nuestras cientos de transacciones cotidianas con empresas, organismos de gobierno, proveedores de servicios o cualquiera con quien intercambiamos un dato en forma digital, desde un banco hasta el análisis de sangre del laboratorio que nos llega por *mail*. Todo está allí. Cada dato está en un sitio preciso, vive y duerme en un lugar como ese. Pero casi no sabemos dónde están físicamente los centros de datos. Como dice el periodista Andrew Blum en su libro *Tubos*, los *datacenters* parecen seguir la regla de los combates de la película *El club de la pelea*: «La primera regla de los centros de datos es que no hay que hablar de los centros de datos».

En Ringo todos son hombres. Cuesta verlos: están entre los pasillos, dentro de cuartos armando conexiones, detrás de una pantalla monitoreando el funcionamiento de los datos. Cada tanto, alguno sale de su lugar, pasa rápido por detrás de una columna, se vuelve a perder detrás de un enjambre de cables. Cada grupo tiene sus rasgos. Los ingenieros, el grupo más pequeño, se visten de camisa y pantalones de

color claro, más livianos que un *jean*, menos pesados que un traje. Son los más sofisticados, miran un poco más de lejos, sonríen, charlan. Los ingenieros más jóvenes o los técnicos que ocupan los puestos detrás de las pantallas en el centro de operaciones del edificio, usan *jean* y remera; los más formales, una chomba y un suéter. Son los nerds, los que se pasan el día chequeando que los datos circulen en orden, cada tanto entran a revisar un servidor, pero su mundo consiste en una fila de pantallas, una pegada a la otra. Y está el grupo de Leandro, los técnicos electrónicos, electricistas o mecánicos, los que «meten mano», los duros, los peso pesados del *datacenter*. Su uniforme es el azul desgastado, casi gris, del pantalón de tela gruesa Pampero y una chomba del mismo color con el logo de la empresa.

—Igual acá todos hacemos un poco de todo, desde los cálculos hasta ajustar tuercas —dice Leandro, con la ceja derecha, gruesa y oscura, levantada, mirando de costado, mientras abre otra puerta.

En la primera habitación, está la conexión con los brazos de internet que llegan desde la calle. El cuarto está casi a oscuras, pero alberga un tubo grande que resalta por su tamaño. En la jerga se llama «tritubo», es decir, un tubo triple, de quince centímetros de diámetro, que viene desde debajo de la vereda y entra en el edificio cargado de la información que compone la Red. Mientras el cable hace su recorrido y entra en este cuarto, nada se detiene adentro suyo. Internet, puesta en un dibujo sobre un mapa, forma anillos. Si no llega por una ruta, lo hace por otra. Y por eso, aquí, en los centros de datos, todo está duplicado: dos salas para servidores, dos equipos de energía, dos sistemas antiincendios, dos tanques de agua. Con uno, todo funciona. Pero el otro siempre está dispuesto en caso de emergencia: la falla de un servidor, un corte de luz, un incendio.

El tritubo, que llega cargado de cables en su interior, entra directamente en un *rack*, una fila apilada de servidores donde se guarda, se intercambia y se le da energía a los datos. Ya estamos en la segunda sala, la de los servidores. En general, no hay problemas, pero los clientes —no solo los individuales, sino las compañías, bancos o empresas de contenidos que confían su información al proveedor de internet— pagan justamente para que su información siempre esté resguardada. Por eso, para que ninguna falle, cada servidor tiene dos bocas de alimentación eléctrica. Si falla, también están en juego nuestros datos más íntimos, nuestras vidas y almas digitales. Los *datacenters*, en su asepsia blanca y fría, por momentos nos hacen olvidar que dentro de sus paredes pasan sentimientos y pensamientos. Que dentro de ellos estamos nosotros, a través de nuestras células de información que circulan por sus venas.

Los servidores son todos parecidos, casi clones. Estanterías de metal negro con bandejas cubiertas de luces que titilan sin descanso. Si esos heraldos de los microdatos nos contaran cómo es el lugar donde trabajan, nos dirían que en los *datacenters* es difícil estar cómodo, que es invierno, verano, invierno, verano otra vez. El recorrido es de confort e incomodidad. Porque, dada la cantidad de energía

que emplean, los centros de datos están diseñados con un esquema que se repite: un pasillo frío, un pasillo caliente, intercalados. En uno, los servidores reciben un baño de aire acondicionado helado, para evitar que se recalienten con la electricidad. En otro, el clima es opuesto: los equipos desechan el aire ya usado que sumó la temperatura del trabajo del intercambio; ya caliente, el aire es reabsorbido por el sistema para refrigerarse.

Mientras eso sucede, siempre hay ruido, el de internet demostrando que nunca deja de moverse. Es el pulso del monstruo que se calma al volver a la calle, cuando las conexiones vuelven a quedar aisladas en su fortaleza privada inmune a incendios y cortes de energía. El alivio es instantáneo. Al volver al mundo, regresa el silencio del *wifi* y las máquinas de la internet real permanecen tras sus muros.

Entonces aparece un servidor distinto. Desde adentro, lo bañan luces de azul eléctrico que lo destacan frente al resto. En el frente, un logo grande de EMC2**[39]**, uno de los fabricantes más conocidos de aparatos y *software* de almacenamiento de información. Leandro sabe que tiene que explicar la magia de ese tótem.

—Es un servidor de un banco. No te puedo decir de quién, pero es importante. Cada lucecita guarda datos de 250 clientes. Y cada uno de ellos puede almacenar 300 gigas. Pero, en realidad, ¿sabés que es esto? Lo que la gente llama «la nube». La nube es un aparato como este, donde cabe un montón de información.

Con el puño cerrado, Leandro le da un golpe suave pero firme al servidor cubierto de azul. Es un golpe de amistad: él lo conoce por adentro; yo no puedo verlo. Y también de fortaleza: en su interior, rodeado del esqueleto de metal y la llave maestra que solo tiene el cliente, hay algo que necesita ser protegido.

—Igual, yo mismo a veces me creo la historia de la nube. Cuando camino por el *datacenter* con la laptop, midiendo algo, y mientras tanto contesto *mail*, yo también tengo la sensación de que internet «está en el aire», aunque sepa que no es tan así. Pero, para los clientes, «la nube» es sinónimo de confianza. Y también se usa para no explicar la complejidad de todo esto.

Según un estudio de Greenpeace de 2010**[40]**, el 2 % de toda la electricidad mundial nos lleva a los centros de datos, que aumentan su consumo en un 12 % cada año. Solo en este edificio hay una capacidad de 13 200 watts. Pero con la mitad de esa capacidad se sostiene su funcionamiento. La otra mitad es una reserva, ante posibles cortes, que pueden durar hasta 12 horas sin perjudicar los datos de los clientes. La capacidad es tan grande que solo alzando la cabeza hacia arriba, una sola barra de enchufes de una de las salas cuenta con 6 mil amperes. Esto permitiría mantener encendidos 6 mil televisores o 12 mil computadoras. Si el sistema fallara, existen dos grupos electrógenos de 1400 kilovoltioamperios (KVA), una cantidad de energía tan grande que permitiría mantener encendidos, al mismo tiempo, 5600 equipos de aire acondicionado de tres mil frigorías. Para poner en marcha los grupos electrógenos en este *datacenter* hay 4 mil litros de gasoil, una cantidad con la que un

auto promedio podría recorrer 60 mil kilómetros, lo que equivale a una vuelta y media al mundo.

Con los equipos funcionando sin pausa las 24 horas, el riesgo de incendios existe y tiene que ser evitado. En la sala de prevención hay dos bombas de agua que funcionan cada una con motores de 75 caballos de fuerza, una energía capaz de mantener funcionando 300 lavarropas a la vez. Con esa fuerza, ante un episodio de fuego, podrían derrarmarse, en una catarata gigante, 40 mil litros de agua, cantidad suficiente para realizar 600 lavados en un lavarropas moderno.

Los *datacenters*, aunque no suceda habitualmente, se incendian. A fines de 2013, sucedió con el de Telecentro, en San Justo, provincia de Buenos Aires. Los equipos se sobrecalentaron, hubo problemas de refrigeración y sobrecarga eléctrica y se produjo un incendio que dañó el 80 por ciento del sistema eléctrico. Gran parte de los clientes de la empresa fueron afectados y los técnicos tardaron meses en restablecer el servicio.

Pero en Parque Patricios la mañana está en calma. Camino a la última sala, espiamos un laboratorio de pruebas. En una sala cerrada, también blanca pero repleta de cajas con equipos recién llegados de China, hay cuatro hombres, del grupo de los nerds, tocando botones y ajustando detalles de módems ZTE (una de las marcas más populares del mundo). Como robots que salen por un momento de su obsesiva tarea, se convierten en humanos y salen por un momento de su concentración. Se sorprenden de las visitas, no habituales en esta parte del *datacenter*, nos saludan y nos explican cómo, en estos planos y pantallas, están simulando la distribución de una nueva tecnología de fibra óptica en una manzana de la ciudad de Buenos Aires. Ya apasionados, explican cómo, con estos aparatos, se podría llevar internet a 4 mil clientes, en 10 kilómetros. Pero para eso, la teoría que ellos arman tiene que volverse real: salir a la calle, a los edificios, romper veredas, negociar un espacio en un sótano y así recorrer el camino del progreso, donde las neuronas de internet viajen cada vez más rápidas para llegar a otras, en otro extremo de la ciudad.

En la siguiente sala, nos queda la última parte de los servidores, tan caótica como repleta de problemas para el futuro. Son los que generan las interconexiones entre distintos servidores de la misma empresa o con los servidores de otra compañía. Cuando se conectan con otros, estamos ante una interconexión.

Las interconexiones son una parte fundamental de los centros de datos y de la Red, ya que vinculan, en un camino directo, la información de una empresa con otra. Por ejemplo, pueden conectar los servidores de un proveedor de tránsito de internet, como Iplan, Speedy o Fibertel, con un proveedor de contenidos como Facebook o Netflix. El objetivo de estas interconexiones es hacer que el tránsito entre los dos destinos recorra menos distancia, y por lo tanto, lo que se esté intercambiando entre un destino y otro llegue más rápido, se vea mejor o tenga mejor calidad. Cuando hablamos de redes, también hablamos de estas conexiones cruzadas que suceden,

justamente, en los centros de datos. Y son tan importantes que a veces hay espacios destinados solamente a ellas.

Las interconexiones se negocian en acuerdos llamados *peering* y también se hacen con empresas que ofrecen contenidos como Google o Facebook. Son acuerdos complejos que pactan primero las empresas, luego los ingenieros de redes y finalmente se activan después en rutas físicas concretas, existentes o nuevas. Pero no son solo acuerdos. Como dice Andrew Blum en su libro *Tubos*, «eso sería decir que la política es meramente la actividad de gobernar». La realidad es que se negocian desde el poder y el tamaño de cada compañía (a más grande, más capacidad de negarse a conectarse a una red o a cobrar por hacerlo) y cada empresa elige su política: algunas tienen *peering* abierto y otras son más selectivas. Pero otras veces, los acuerdos no son tan sencillos. Allí internet deja de ser solo física y se transforma en política. Allí empieza a afectar aún más nuestras vidas, que quedan en el fuego cruzado de los poderosos de internet. Allí la concentración se hace más real. El mapa se traslada a las negociaciones, las leyes, los *lobbies*, los acuerdos. La guerra se vuelve real.

La guerra por la neutralidad de la Red es económica y de regulación de la infraestructura. Se libra entre los dueños de internet, pero sus batallas pueden afectar nuestra vida diaria de una forma muy directa.

Desde que internet es un servicio tan básico y necesario como la electricidad, los prestadores de servicios de internet adquirieron un poder inmenso. Sin ellos no existirían las rutas para realizar cualquier actividad de una Red que en los últimos años necesitamos cada vez más y para todo. Ya no nos conectamos solo para ver videos, para chatear o para mandar un *mail*: las ambulancias y los quirófanos se conectan para enviar información sobre un paciente; los bancos y las empresas envían y reciben información de sus clientes que toman decisiones minuto a minuto; los gobiernos nacionales y locales utilizan la Red para brindar servicios a sus ciudadanos; los niños y jóvenes se valen de ella para estudiar… y así con cada esfera de la vida.

Nos volvimos internet-dependientes. Y a medida que necesitamos cada vez más capacidad de infraestructura para conectarnos, las empresas que la proveen empiezan a reclamar.

La neutralidad es un principio que rigió la Red desde su nacimiento y fue respetado durante un tiempo. Se basa en que los proveedores deben dar acceso a cualquier contenido de la web sin privilegiar a uno por encima de otro. Según esta regla, para las máquinas conectadas todos los paquetes son iguales: no «mira» qué hay adentro (si es una foto, un texto, una canción) sino que simplemente transporta los bits hasta su destino. De acuerdo con este principio, el usuario no tendría que notar diferencia si navega en dos páginas o si descarga dos archivos iguales al margen

de donde provengan. Si dos archivos pesan lo mismo deben ser tratados de la misma manera sin importar el origen. Tampoco tendría que notar diferencia entre navegar o hacer una llamada por Skype, o entre ver un video en YouTube, en Netflix, en Cuevana o en Popcorn Time. También implica que debemos tener acceso a absolutamente todas las páginas disponibles en la web. En una red neutral, si queremos ver o leer algo, podemos hacerlo.

La neutralidad es importante por muchas razones. Primero, porque garantiza la igualdad de los contenidos, por lo tanto, la libertad de expresión. Evita que haya contenidos de primera clase y de segunda. Se suele decir que internet trajo una «democratización» a varios aspectos de la cultura. Si bien esto es discutible[41], es cierto que en la Red hay muchísimas más opciones para informarnos de algo o conocer distintas opiniones. Si no existe una Red neutral, la libertad de información y de expresión se ve limitada. Segundo, por razones de privacidad, ya que impide a los proveedores de contenidos «mirar» lo que estamos intercambiando o consumiendo los usuarios. Sin neutralidad, los proveedores de acceso tendrían que acceder a los datos para saber quién se conecta a qué y desde dónde.

Sin embargo, desde hace algunos años hay intentos de romper este principio de neutralidad. La forma más común de hacer esto sería (y está comenzando a suceder) que las empresas que ofrecen acceso a internet realicen acuerdos con los proveedores de contenidos (por ejemplo, que Fibertel haga un acuerdo con Netflix o Speedy con YouTube) para que sus datos viajen más rápido para los usuarios que contratan sus servicios en detrimento de los que tienen otro proveedor. En este escenario, el primer riesgo sería que los grandes proveedores (tanto de acceso como contenidos) acapararen cada vez más tráfico, limitando la posibilidad de nuevos actores o empresas de posicionarse en el mercado.

¿Por qué, entonces, hubo intentos de limitar la neutralidad? «El inicio de toda esta discusión tiene que ver con el congestionamiento de tráfico. Internet siempre tuvo congestionamientos en algún lugar de la red. Internet está todavía en pañales. Va creciendo exponencialmente y ese crecimiento siempre genera problemas en algún lado, que se van solucionando sobre la marcha. Siempre hubo crisis de crecimiento y hasta ahora para el usuario siempre ha sido transparente, nunca le produjeron ningún efecto. Hay que buscar soluciones que no rompan con la neutralidad», explica y propone Sebastián Bellagamba, director regional para América Latina de la Internet Society[42]. En efecto, cada vez usamos más nuestras conexiones a internet, no solo para navegar por la web, sino para realizar una serie de actividades diarias como mirar televisión *online*, jugar, chatear, mandar mensajes de voz o videos, o consumir toda clase de entretenimiento desde el celular (desde videos y películas, hasta música en *streaming* y comunicaciones locales e internacionales), conectar todo tipo de dispositivos del «hogar inteligente», desde *smart tvs*, hasta cafeteras, relojes, radios y cualquier elemento de la llamada «internet de las cosas» que requiera conectarse a la Red para funcionar. En América Latina, todos los años se incrementan las horas que

las personas miran televisión y video en dispositivos portátiles (laptops, tabletas y *smartphones*), que llegan a un promedio de 8,2 horas en *smartphones* y 4,9 horas en tabletas, principalmente en países como Brasil, México y Chile[43].

La cuenta es sencilla: si cada vez necesitamos más ancho de banda —o más «caño»— para satisfacer nuestra demanda, los proveedores de internet tienen que incrementar la inversión. Tienen que darnos más, para poder consumir más. Pero entonces, estos proveedores de tránsito se plantan frente a los proveedores de contenido y les dicen (en un diálogo imaginario): «Si la gente cada vez necesita más conexión para ver sus contenidos, como películas o juegos *online*, subir fotos a las redes sociales o hablar sin costo extra con su amigo que vive lejos a través de internet, ¿por qué ustedes, que ganan dinero con sus servicios, no se hacen cargo de este costo? Y, si no se hacen cargo, ¿por qué los proveedores no podemos cobrarle más a quienes más utilizan la Red?». Allí radica el conflicto central de la guerra por la neutralidad. Por eso, los proveedores de acceso son los más interesados en que se vulnere este acuerdo. Un intento, aunque solo fueron declaraciones, sucedió en 2006 cuando compañías como Cisco y Motorola propusieron establecer tarifas de diferente categoría: platino, oro, plata y bronce, según las necesidades de cada cliente. Estas megaempresas argumentaban que se trataba de adaptar mejor el acceso según el tipo de usuario. El debate se ha abierto también con los servicios de voz sobre IP, como Skype. Si se erradicara la neutralidad de la Red, los proveedores de conexión podrían evitar tanto el acceso a este servicio si lo creyesen oportuno como la descarga de contenidos por *peer to peer* o la mensajería instantánea.

Según Neil Irwin, columnista de tecnología de *The New York Times*, el debate sobre la neutralidad encuentra una respuesta real si nos hacemos la siguiente pregunta[44]: ¿internet es como la electricidad o como la televisión por cable? Si es como la electricidad, es decir, un servicio básico para nuestras vidas, sin el cual ninguna actividad económica ni cotidiana es ya posible, entonces tenemos que defender la neutralidad. Si consideramos que es como el cable, en cambio, entonces estamos a favor de establecer distintos tipos de tarifas según la «cantidad de internet» (es decir, de caños, de espacio en la Red) que usemos, de igual forma que pagamos más si queremos suscribirnos a más oferta de canales o a paquetes *premium* de deportes o de películas.

Durante un tiempo, hasta 2010, pero más aún después de 2013, la guerra de la neutralidad permanecía oculta. Casi todos, usuarios, gobiernos, empresas, se declaraban a favor de una «internet abierta». Pero lo cierto es que el consumo de contenidos, especialmente de películas y datos móviles, incrementaba cada vez más un uso intensivo de la Red. Lo que era antes una declaración de principios chocaba contra la necesidad de inversiones cada vez más grandes para soportar el uso creciente de internet. Los dueños de los caños y los cables, es decir, los proveedores de internet, mayormente empresas telefónicas o de cable —según los países[45]—, se enfrentaban con este tema. ¿Cómo hacían para dar servicio a esa demanda cada vez

más grande? La respuesta: invertir más. Pero entonces llegaba el conflicto: si las responsables del mayor consumo son las empresas de contenidos, con Netflix y las compañías que ofrecen contenido de entretenimiento vía *streaming* a la cabeza, ¿por qué la inversión tiene que ir por cuenta de los proveedores de internet? Esa guerra, que es la guerra entre proveedores de tránsito y de contenidos, es la que está detrás del debate. Y la que, durante 2012 y 2013 enfrentó con uñas y dientes a Comcast, la mayor proveedora de cable e internet de Estados Unidos, con Netflix, en una disputa que llegó a la Comisión Federal de Comunicaciones. La guerra se mantuvo en la esfera de una disputa entre privados, con batallas judiciales frecuentes pero a las que prestaban atención los ejércitos de las telecomunicaciones, algunas empresas de internet y los grandes estudios de abogados que luchaban por ganar terreno en cada combate.

Hasta que el 10 de noviembre de 2014 Barack Obama se pronunció: «Una Red abierta es esencial para la economía estadounidense y, cada vez más, para nuestro modo de vida. Al abaratar el coste de lanzar nuevas ideas, favorecer la creación de movimientos políticos y acercar a diferentes comunidades de personas, se ha convertido en una de las influencias democratizadoras más importantes que hayamos conocido nunca». Con esto, el Presidente de Estados Unidos se puso del lado de declarar internet como un servicio público, como la electricidad. Sin embargo, no todos los líderes del mundo coinciden: la canciller de Alemania, Angela Merkel, cuyo gobierno tiene una gran cercanía con el sector de las comunicaciones, se pronunció a favor de una internet de «dos vías». Esto implicaría una internet «rápida», donde los proveedores podrían bajar el acceso a servicios que no hayan pagado un extra para ser tratados como «*premium*».

Más allá de las posturas internacionales, el tema de la neutralidad requiere de decisiones locales[46]. De leyes donde cada país declare la neutralidad[47] y a partir de esa posición tenga capacidad de regular a los proveedores de infraestructura para garantizar un mismo acceso a todos los contenidos. Hoy es casi un consenso mundial la «defensa de la neutralidad de la Red». Es casi políticamente correcto decir que uno está a favor, como lo estaría de la paz mundial, de la salud o la educación gratuita. Claramente, debemos defenderla. Sin embargo, las discusiones y, sobre todo, las definiciones que la sostengan, dependen de enfrentamientos económicos entre empresas de sectores tan poderosos como las telecomunicaciones, la tecnología y los medios de comunicación. Por eso, la decisión final siempre es política. Y local.

Mientras tanto, en el país donde nació internet y donde se concentran gran parte de los operadores con las mayores infraestructuras, el presidente Barack Obama le propuso a la Comisión Federal de Comunicaciones que clasifique la conexión a internet como un servicio de comunicación básico y con esto garantice la neutralidad. Pero tampoco el desarrollo de la Red en ese país estuvo libre de batallas. Al contrario, su historia y su futuro siempre fueron de la mano de otras guerras, miedos y amenazas.

Segunda parte

De la bomba atómica a Snowden: Cómo el miedo construyó la Red.

IV

El dilema de internet: utopía científica versus intereses corporativos

> «La tecnología lleva una doble vida: una se acomoda a las intenciones de los diseñadores y a los intereses del poder, y otra los contradice, actuando a espaldas de sus arquitectos hasta provocar consecuencias y posibilidades inesperadas».
>
> DAVID NOBLE.
> *Forces of production* (1984).

> «En vez de perseguir la política con política, los científicos la buscaron por otros medios. La ciencia no es política, sino política por otros medios».
>
> BRUNO LATOUR.
> *La pasteurización de Francia* (1998).

El 22 de octubre de 1962, Estados Unidos emitió la máxima alerta posible en la historia en su sistema de seguridad: la Defcon 2. Para su ejército, era la orden de prepararse para defender su territorio contra una guerra nuclear. El líder de la Rusia comunista Nikita Kruschev había aprovechado la fallida invasión a Bahía de Cochinos por parte de Estados Unidos para ordenar la instalación de una parte de su arsenal nuclear en las costas de Cuba, con el apoyo de su aliado y flamante héroe de la Revolución, Fidel Castro. Y así se desataron los días más calientes de la Crisis de los Misiles, el episodio que llevó a la Guerra Fría a su punto límite.

Tras varios días de negociación, el presidente norteamericano, John Fitzgerald Kennedy, llegó a un acuerdo con Kruschev y logró el objetivo más importante de cualquier ocupante del poder en la Casa Blanca: mantener la *homeland security*, es decir, su territorio, libre de intrusos. Hasta entonces, las guerras siempre habían estado lejos del país, pero durante ese octubre los misiles instalados en isla del Caribe habían estado a 200 kilómetros de pisarle los talones al suelo de Florida. En esas playas de casinos y lujo, James Bond transformaba la realidad en la saga más popular de la época. Sus enemigos, los espías soviéticos, eran los villanos de la Guerra Fría. Una combinación de secretos, conspiraciones y miedos dominaba la época.

Pasada la Crisis de los Misiles, Estados Unidos se encontraba nuevamente a salvo y vivía un período de optimismo cultural, producto de la prosperidad económica posterior a la Segunda Guerra Mundial. El pop, el *rock* y las series de fantasía y familias perfectas se comenzaban a multiplicar por el mundo a través de un invento reciente: la televisión. En la Argentina, eran tiempos de progreso social, con una juventud que por primera vez iba a la universidad masivamente, familias que compraban su primer auto y aparato de televisión, versiones del *rock* en español con bandas locales y un florecimiento del arte vanguardista. La ciencia y la industria no se quedaban atrás: Bernardo Houssay, premio Nobel argentino, dirigía el recién fundado Consejo Nacional de Investigaciones Científicas y Técnicas (Conicet) y las empresas nacionales invertían en sus primeros centros de investigación y desarrollo.

Pero en el mundo, sobre todo en Estados Unidos, la amenaza seguía siendo inminente. Una bomba, además del inicio de la Tercera Guerra Mundial en su territorio, podía suponer la incomunicación del país con el resto del planeta. La infraestructura de telecomunicaciones ya estaba concentrada en manos de unas pocas empresas y suponía que un corte en cualquiera de sus rutas se transformaría en un desastre. ¿Cómo sobrevivir a ese ataque? El Departamento de Defensa de los Estados Unidos se estaba haciendo esa pregunta desde fines de los 50 cuando apareció en escena Paul Baran. Este ingeniero eléctrico de cachetes grandes y anteojos gruesos, nacido en Polonia en 1926, emigrado y educado en Filadelfia, les ofreció una solución.

Y así nació internet. Del miedo. Lo sabían los científicos que la crearon en los 60 y lo saben todavía quienes hoy tienen que defenderla de las nuevas amenazas. La historia de la Red es una historia de guerras.

Financiado por la Rand Corporation, un centro de investigación orientado a los avances militares, Paul Baran desarrolló una idea que hoy parece pequeña pero fue revolucionaria: el *packet switching*[48]. La conmutación de paquetes era una forma de red de comunicaciones distribuida y basada en la redundancia: si alguna de sus partes fallaba o era destruida en un ataque, los paquetes simplemente encontraban otra ruta para seguir adelante y llegar a destino. Su gran innovación fue romper la concentración de la información y dispersarla para dividir los riesgos. La información podía ser fragmentada: se podía dividir un mensaje en partes pequeñas antes de arrojarlo a la red y luego volver a unirlo al llegar a su destino. Así lo explicaba el propio Baran: «Me interesaba el concepto de las "redes neuronales" y encontré una investigación sobre el cerebro que explicaba que, cuando nos ponemos viejos y no encontramos una palabra, una serie de neuronas tienen la función de encontrar un sinónimo que la reemplace. Esa idea me inspiró a diseñar mi sistema».

En 1969, tres meses después de que un humano llegara a la Luna, la idea se transformó en acción. Con la ayuda de la Universidad de California, el 29 de octubre

a las 22.30 en Santa Mónica se conectaron los primeros nodos de Arpanet[49]. Fue la primera forma que adaptó este invento que luego mutó, creció y que se diseminó en el planeta como internet. «Sí, el origen de la *conmutación de paquetes* es la Guerra Fría. Teníamos que ser capaces de resistir un ataque. Podía pasar o no, pero si no podíamos resistir a eso estábamos limitados», explicó luego Paul Baran, confirmando el mito de origen de internet en el miedo a una ofensiva nuclear. Arpanet, como muchos de los avances provocados por la inminencia de una catástrofe o una necesidad política, fue un descubrimiento provocado por una necesidad más que una invención racional. Y una confirmación de la segunda ley de la tecnología del historiador Melvin Katzenberg: «La invención es la madre de la necesidad[50]».

Arpanet fue la columna vertebral de internet hasta 1990. Tantos actores fueron parte de su desarrollo que no sería posible en un concurso de preguntas y respuestas dar un solo nombre para la consulta: «¿Quién inventó internet?». La Red no tiene un padre, sino muchos. Fue producto de una serie de hombres que sumaron esfuerzos, eslabones de una cadena. Con ese trabajo en equipo, en septiembre de 1973 Arpanet ya cruzaba América y llegaba al University College de Londres. La conexión Estados Unidos-Inglaterra replicaba la misma dupla de países que había recorrido la instalación inicial del telégrafo, con la diferencia de que en el caso de internet Nueva York todavía aparecía casi desconectada. En esos años, hacia finales de los 70, la flamante Red se expandía alrededor de cuatro regiones: Silicon Valley y Los Ángeles al oeste del país; Boston y Washington, al este. El mapa no era casual ni antojadizo: aquellos eran los epicentros universitarios y militares del país.

Internet ingresó en la adolescencia en 1983 con la invención de una serie de protocolos que le otorgaron al monstruo un alfabeto común, un lenguaje propio. Sucedió cuando los ingenieros de *software* Vint Cerf y Bob Kahn[51] le dieron vida al protocolo TCP/IP, que se convirtió en el idioma de la Red. Con él, las máquinas tuvieron un código común para intercambiar información bajo una serie de estándares que permiten que computadoras y dispositivos de distintos fabricantes, con distintos sistemas operativos, se comuniquen entre sí y dialoguen. Fue un cambio conceptual muy importante: ya no eran solo unas computadoras conectadas, sino que las distintas redes ahora tenían la capacidad de *charlar* unas con otras. Cada una podía decidir, con lo cual el sistema perdía su centralidad.

Mientras la Red avanzaba en estándares técnicos comunes, se crearon las primeras organizaciones para el manejo de internet. En 1986, se estableció la Fuerza de Tareas de Ingeniería para Internet (IETF), que desde entonces administró la evolución técnica de la Red. Su tarea era y sigue siendo la regulación de los estándares, conocidos como RFC[52]. Fue el primer organismo para la administración de internet, al que en la década de los 90 se agregarían otros.

En 1989, otro gran avance impulsó a la bestia: el lenguaje HTML[53], que permitió el nacimiento de la *World Wide Web* o «la web» a secas, al permitir la interconexión de un universo de sitios hasta entonces desparramado a través de navegadores. Creado por el programador inglés Tim Berners-Lee en el CERN (Organización Europea para la Investigación Nuclear), ese otro idioma fundamental permitió una forma sencilla de publicar información en la Red, a través de una estructura que permitía incorporar, además de texto, otros elementos a las páginas, como imágenes y video, y unirlos a través de links dentro del mismo sitio o de páginas externas. Desde entonces fue mucho más fácil navegar, saltando de un documento a otro a través de un clic.

La estandarización del protocolo TCP/IP primero y la web de Berners-Lee, después, impulsaron un crecimiento exponencial de la Red en los años siguientes. Pero además lo hicieron sobre la base de un esquema abierto, en el que se basaron los futuros desarrollos de internet. Si «el código es la ley de internet[54]», estos dos avances configuraron un modelo futuro de la Red basado en la filosofía de «lo abierto», en compartir para avanzar. De allí en más, las computadoras dejaron de ser aparatos aislados, cerrados en sí mismos, para formar parte de un gran océano interconectado.

En los 80, en la escuela primaria, quienes teníamos la entonces avanzada asignatura de Computación, usábamos las máquinas para jugar y para hacer algunos ejercicios de programación básicos. En un aula cruzando el patio de la Escuela de Lenguas Vivas, cerca del bosque de la ciudad de La Plata, los viernes me sentaba con otros chicos en unos bancos alargados, dispuestos en filas enfrentadas a los aparatos, entonces pesados y grandes. Cada uno recibía una consigna para hacer una figura en Logo, un lenguaje de programación más popular en la época. La clase consistía en avanzar en una operación matemática y apagar la computadora hasta el siguiente encuentro. En el secundario, a principios de los 90, la novedad era aprender a utilizar el sistema operativo Windows y sus, al parecer, infinitas posibilidades, en especial el procesador de textos Word y las hojas de cálculos del Excel. Pero todavía cada uno trabajaba solo, en su máquina. Hasta que un día de 1996, un profesor altísimo de botas texanas e higiene dudosa hizo algo distinto: conectó una computadora a un módem y tras su chirrido doloroso y metálico, abrió las puertas de internet. El pasaje hacia el ciberespacio (por entonces una idea de la ciencia ficción, conformado por una serie de prehistóricas páginas de museos, alguna enciclopedia incompleta y unas portadas de diario que tardaban eternidades en cargarse) se consumaba a través de Netscape, el navegador más moderno de la época, el mismo que utilizábamos en mi casa para conectarnos a la web en familia, por unos minutos y en turnos.

Lo primero que había que hacer era crearse una cuenta de *mail*. Gmail aún no era ni un sueño lejano. Yo elegí Yahoo, mi hermana Hotmail y mi mamá configuró el Outlook con una casilla familiar que fusionaba su nombre con el de mi papá. En los orígenes, el intercambio era entre nosotros, nuestros tíos del sur, las amigas de mi

mamá emigradas, mensajes llenos de colores, tarjetas navideñas y *mails* con forma de cartas que empezaban siempre con un formal «Querida Natalia». Entonces no sospechábamos que aquellas puertas (virtuales) no se cerrarían más. Que la Red crecería en el mundo y en nuestras vidas hasta adquirir el mismo estatus que el de la electricidad.

Cuando Berners-Lee desarrolló en código HTML, hizo algo también muy importante: en vez de patentarlo y cobrarle por su uso a todos en un futuro —lo que lo hubiera ubicado en el primer puesto de millonarios de *Forbes*—, lo liberó al dominio público. Cualquiera podía usarlo sin pagarle. Con esto, siguió los pasos de sus predecesores para que internet continuara creciendo como una invención colectiva. La web se expandió mundialmente sobre una estructura de lenguajes y protocolos que permitía que cualquiera pudiera crear sitios y aplicaciones bajo un idioma común.

Hoy, 25 años después de aquel estallido, gran parte de ese modelo se mantiene. Cualquiera puede sumar su aporte a la Red simplemente subiéndose a los estándares o creando sobre lo que ya está algo nuevo. Esa es una de sus grande potencialidades: para estar en internet solo se necesita una conexión, querer ser parte y contribuir. Casi el 70 % de los prestadores de servicios de internet (conectividad, servidores que alojan sitios web, webmails y otros servicios) utilizan en sus máquinas *software* libre que permite usarlo, modificarlo, copiarlo y distribuirlo libremente, ya que su código fuente (el manual de instrucciones o el genoma de cada programa) está a disposición de cualquier persona, empresa u organización. Pero no solo fue adoptado por el poder que esto implica para mejorarlo. También se demostró que es una forma técnicamente estable y segura para la Red y para manejar la información que circula en sus servidores.

El surgimiento de internet fue desde y para un país determinado, Estados Unidos. Pero el modelo abierto y distribuido hizo que la Red dejara de tener una sede geográfica real. Sería imposible hacer un mapa completo de ella que muestre gráficamente todas sus interconexiones[55], porque están literalmente en todo el mundo. La Red fue un invento verdaderamente mundial, el primer hijo colectivo de la especie humana, que creció en los mismos años en que se empezaba a utilizar la palabra globalización, a principios de la década del 90. En esa época, también nacieron varias instituciones de gobierno supranacionales, destinadas a ordenar problemas que se salían de las fronteras (la Organización Mundial del Comercio, la Corte Penal Internacional, por ejemplo). Los Estados cedieron parte de su soberanía para ser partes de un todo que los superaba y donde internet era la forma dominante de acortar las distancias. Como dice el sociólogo español Manuel Castells, se convertía en la tecnología decisiva de la Era de la Información, como antes la electricidad había sido el vector tecnológico de la transformación de la Era Industrial[56].

En 1996, la primera vez que se calculó el número de usuarios de internet, éramos 40 millones. En 2014, llegamos a casi 3000 millones, en 194 países, aunque la mayoría de ellos viviendo en China. El desarrollo de las tecnologías inalámbricas, a principios de los años 2000, permitió otra expansión: que internet llegara a lugares del mundo donde antes había sido muy caro (o poco rentable) instalar infraestructuras de telecomunicaciones. Explosión tras explosión, la Humanidad se conectó casi por completo.

La imagen de las dos fuerzas en contradicción, lo abierto y lo cerrado, lo distribuido y lo vertical, continúa siendo parte del ADN de internet. En su libro *The Master Switch*, Tim Wu, profesor de medios y tecnología de la Universidad de Columbia[57], dice que siempre hay dos fuerzas subyacentes en la tecnología. Unas, las de apertura, están generalmente asociadas al nacimiento de esta, cuando los entusiastas hacen y deshacen casi con espíritu *amateur*. Las otras, de concentración o cierre, se relacionan con el uso masivo y el crecimiento comercial de las tecnologías. Pero las dos, sostiene Wu, se necesitan, porque su combinación y fluctuación permanente es la que genera los acontecimientos. Lo cerrado surge como respuesta a lo abierto. Pero lo abierto luego disputa los espacios concentrados.

La historia de internet avanzó sobre esos dos procesos en principio contradictorios, pero intrínsecamente complementarios.

Entre los 60 y los 90, la necesidad política combinada con el avance tecnológico (de las telecomunicaciones y la informática) promovió la cooperación de la corporación militar con universidades, científicos y agencias estatales, en un proyecto fundamentalmente abierto y público.

En la segunda parte de su historia, desde mediados de los 90, la Red creció sobre un modelo distinto, que centralizó el control de internet. Hubo dos procesos que marcaron la época: la privatización de la Red, que pasó de la financiación estatal a manos privadas; y la creación de una serie de organismos que desde entonces se encargan del gobierno de la Red.

Entonces, nacieron otras batallas que hoy son parte de las guerras de internet: ¿quién debe decidir sobre un bien que todos utilizamos y contribuimos a crear?

En 1994, el presidente norteamericano Bill Clinton decidió trasladar el control de internet del estatal Departamento de Defensa a manos privadas, dejando su manejo en la Fundación Nacional de la Ciencia. El proceso tuvo sus detractores. Para el *New York Times*, la «polémica carrera a la privatización» de la Red era «entregarla a las garras del libre mercado». «La comunidad científica, que hasta ahora ostentaba la titularidad y el uso masivo de la mayor autopista de comunicación, se lamenta de que la Red se vaya desvinculando poco a poco de la investigación para caer en manos de las empresas del sector privado, que saludan esperanzadas la nueva etapa», decía la periodista Ami Harmon[58].

Con una internet expandiéndose en caños, se hizo necesaria la creación de una serie de organismos para coordinar su infraestructura lógica o, como la llaman los ingenieros, los «recursos críticos de la Red». En 1992 se fundó la Internet Society (ISOC), una organización encargada de articular las reuniones y avances de la Internet Engineering Task Force (IETF o Grupo de Trabajo de Ingeniería de Internet). En 1998, se creó la ICANN (Corporación de Internet para la Asignación de Nombres y Números).

LA IETF, la ICANN y la ISOC siguen siendo hoy las tres instituciones fundantes de administración técnica de la Red[59]. Entre ellas (y sus representaciones regionales y locales) se mantienen y desarrollan los cuatro pilares en los que se basa internet para su funcionamiento: la asignación de los nombres de dominio (por ejemplo: www.google.com), la gestión de los identificadores de IP (por ejemplo, 209.85.195.104 una de las direcciones de Google, ubicada físicamente en Mountain View, California), el sistema de los llamados servidores raíz de DNS (*DNS root servers*) y los estándares técnicos que permiten y aseguran la interoperabilidad (que las computadoras o teléfonos móviles dialoguen entre sí más allá de su ubicación, su proveedor de conexión a internet, el sistema operativo 97 o el *software* que utilicen).

La ICANN, una asociación privada sin fines de lucro, tiene su sede en Marina del Rey, California. Su objetivo es la «gobernanza de la infraestructura lógica» de la Red. Una de sus funciones es la distribución de las direcciones numéricas de IP, que sirven para identificar cada dispositivo (una computadora, teléfono, tableta) que se conecta a internet para que el sistema sepa a dónde enviar los datos que el usuario le solicita. Lo hace a través de un organismo que depende de ella, la IANA (Autoridad de Números Asignados de Internet), quien se encarga de este trabajo de distribución de bloques de números IP. Como un almacenero con una libreta que lleva la contabilidad de sus recursos, la IANA anota y reparte las direcciones (que no son infinitas y cada tanto requieren una expansión)[60]. Para ello, cuenta con un organismo regional en cada continente, llamado Registro Regional de Internet (RIR). Ese organismo luego «baja» la asignación de los números entre los proveedores de servicios de internet regionales y locales en cada país. Es una estructura jerárquica, pero necesaria, porque mantiene un orden y un conteo centralizado: cada dirección es única y pertenece a una máquina o dispositivo. Si dos computadoras usaran la misma dirección, se generaría un problema similar al de una carta que llega a un destinatario equivocado porque hay una misma calle con un mismo número, pero en localidades diferentes, y el remitente no lo aclara en detalle.

La segunda función de la ICANN es la gestión del sistema de nombres de dominio. Lo hace asignando nombres más fáciles de recordar para las páginas, que se denominan con una cadena de números muy difícil de memorizar, por ejemplo 209.85.195.104. Acordarnos de cada serie de números de los sitios que queremos visitar sería imposible. Por eso se creó un sistema para que ese número sea reemplazado por un nombre y una extensión, en este caso www.google.com. Hay un

grupo de nombres para los países, llamados «nombres de dominio de nivel superior». Son 252: .ar para Argentina, .br para Brasil, .fr para Francia, etcétera[61]. En el inicio de la creación del sistema, entre 1984 y 1997, este grupo de nombres se delegó a cada país, donde es administrado por la institución correspondiente[62]. Y hay otro grupo de nombres, los dominios genéricos, que entre los más utilizados incluyen el .com (para sitios comerciales), .edu (para educación y universidades), .org (para organizaciones no gubernamentales), .gov (para gobiernos), etcétera. Con el tiempo, también se fueron creando dominios para otras actividades, más vinculadas con lo comercial, como los recientemente inaugurados .music (música), .book (libros), .museum (museos), o .travel (viajes), entre muchos otros. La administración de estos dominios se realiza a través de empresas que pagan un monto a ICANN y luego pueden venderlos a otras empresas o particulares.

La tercera función técnica de la ICANN es la administración de los servidores raíz (o *root servers*), una especie de gran guía telefónica de internet donde figura en qué lugar está cada sitio de acuerdo con su IP. Son vitales, porque ante cada pedido que hacemos en nuestro navegador (web o móvil) para llegar a una dirección, el sistema debe consultar dónde está ubicada alrededor del mundo. Al ser internet un sistema planetario, estos servidores raíz son el genoma de internet, el ADN de las rutas que todos navegamos diariamente. Están distribuidos en 13 colecciones, nombradas con letras de la A a la M. Originalmente, diez de estos servidores se encontraban en Estados Unidos[63] y los tres restantes en Estocolmo (I), Amsterdam (K) y Tokio (M). Esto generó uno de los mitos más difundidos de internet: que Estados Unidos, al controlar desde su territorio la mayoría de los servidores raíz, tiene el mando supremo de la Red e incluso la capacidad de desconectar «su cerebro» si lo decide. En algún punto, esto fue cierto, desde que al ser en su territorio donde se instalaron esos repositorios del ADN de internet, eso le confirió un mayor poder durante un tiempo (compartido con los dos países nórdicos y Japón, también occidentales y capitalistas). Pero también fue consecuencia del desarrollo de internet en un país, Estados Unidos, que se encargó del primer diseño e instituciones para operar y administrar los recursos de la Red.

Sin embargo, con el tiempo y con la creación de organizaciones locales capaces de manejarlos y mantenerlos técnicamente, se fueron instalando réplicas de los distintos servidores raíz en otras partes del mundo, entre ellas América Latina. En Argentina, por ejemplo, existen en Buenos Aires y Córdoba réplicas de cuatro servidores (D, F, J, L), que son operados por la Cámara Argentina de Internet (Cabase). En Montevideo, en la Casa de Internet de América Latina, donde tiene su sede LACNIC (el Registro Regional de Direcciones IP de América Latina y el Caribe), hay una copia del *root server* L. En la enorme extensión de Brasil hay 18 servidores raíz, en Santiago (Chile) existen réplicas de un L y un F; y así en cada país de América Latina (Bolivia, Perú, Ecuador, Colombia, Venezuela, Panamá, Costa Rica, El Salvador, Jamaica, México, República Dominicana). Hay también copias en

islas del Caribe como Dominica y en un punto aislado en medio del océano Pacífico, donde Polinesia Francesa alberga una copia del servidor L. Y así, se pueden encontrar reproducciones en todo el mapa[64]. Aun con esta distribución de *root servers* mucho mayor que en los 90, periódicamente vuelve a darse el debate de instalar no solo una copia sino un servidor raíz original fuera de Estados Unidos, por motivos políticos y de soberanía[65].

Las organizaciones técnicas[66] de internet colaboraron en el desarrollo estructural y comercial de la Red tal como la conocemos hoy. Pero a medida que la Red se iba complejizando fue necesario comenzar a considerar otros factores, que involucraban la regulación del mercado, la política y las formas sociales.

Entre 2003 y 2005, durante las cumbres de la Sociedad de la Información de Ginebra y de Túnez[67], se produjo una batalla que estableció el futuro esquema de administración política de la Red. De un lado, estaban quienes creían que sus funciones técnicas debían mantenerse separadas de las discusiones sobre los impactos sociales y económicos de internet, que ya en esos años comenzaban a percibirse como un ámbito a debatir, regular y proteger. Del otro, se paraban quienes consideraban que no hay decisiones tecnológicas divorciadas de la política, y que, por lo tanto, había que pensar una forma de gobierno de la Red que tuviera en cuenta estos impactos sociales. Esta última posición se impuso y quedó plasmada en la *Agenda de la Sociedad de la Información* de la Cumbre de Túnez. A partir de allí, con el impulso del sistema de Naciones Unidas, se definió la «gobernanza de internet» y se la adoptó como la forma de gobierno que todavía rige a la Red.

En épocas de optimismo democratizador de las tecnologías, era una invitación a que los gobiernos aplicaran, localmente y colaborando con empresas y organizaciones sociales, las políticas para gestionar la Red. Pero también era un triunfo de Estados Unidos y Occidente[68] por un modelo de organización supranacional para administrar internet, donde un organismo global iba a incidir en sus políticas futuras, que involucraran no solo las necesidades de cada país, sino que además tuvieran en cuenta los intereses de empresas privadas, usuarios y todo tipo de organizaciones de la sociedad civil que quisieran incidir sobre la Red.

Adoptada la gobernanza como forma de participación y deliberación para los temas de internet, se pusieron en marcha los Foros de Gobernanza de Internet (IGF), una serie de reuniones, llevadas a cabo en distintos países para que todos los involucrados de la Red dialoguen sobre sus problemas y soluciones. Es decir, para que las guerras se peleen en un mismo lugar.

Para un Estado, una empresa privada y un usuario, internet significa algo distinto. Pero sus decisiones y discusiones tienen que tomarse en conjunto, porque, a diferencia de las resoluciones que puede tomar un Estado (que decide sobre su población y su territorio), las de la Red implican incidir sobre un ámbito mundial bajo

un poder compartido. A nadie le conviene que internet «se rompa», pero cada actor, usándola para distintos fines, genera tensiones que pueden ponerla en riesgo.

El esquema es complejo y propio de las formas de gobierno supranacionales de la globalización: muchos actores discutiendo sobre un tema que los afecta a todos y al mismo tiempo librando batallas geopolíticas a través de sus posiciones. En esto, el manejo de internet es tan difícil como el de otros temas de implicancia mundial, como la paz o el calentamiento global. Los Foros de Gobernanza pueden sugerir cómo debe desarrollarse internet de la misma forma que el Protocolo de Kyoto establece recomendaciones sobre cómo manejar las emanaciones tóxicas de gases de las industrias de cada país para no afectar la capa de ozono. Pero la política concreta, las sanciones y los avances específicos los tiene que resolver cada país y es localmente donde se toman las decisiones que moldean la Red. Claro que hacerlo o no supone no solo afectar al país, sino también al resto del mundo. A tantas soberanías como soportes, a tantos usuarios como culturas.

Pero gobernar internet es especialmente complejo porque las instituciones deciden también sobre una de las industrias más millonarias del mundo. Las empresas de contenidos como Google, Yahoo y Facebook, que hoy concentran grandes flujos de información y datos de la Red, se transformaron en grandes actores de poder económico y político.

En 2007, el 50 % del tráfico de internet se consumía a través de cientos de miles de sitios dispersos por el mundo. En 2009, ese mismo porcentaje pasaba solo por 150 sitios. Cinco años después, en 2014, la mitad del tráfico mundial de la Red se concentraba en 35 sitios que ofrecen cada vez más servicios y aplicaciones y a los que confiamos la mayor parte de nuestro tiempo, consumos y datos. Entre ellos, los cinco más grandes tienen una presencia descomunal. De los 3000 millones de usuarios navegando por internet en el mundo en este momento, hay 368 millones conectados a algún servicio de Google, 317 millones a uno de Microsoft, 260 a Facebook, 201 a Yahoo y 164 Amazon**[69]**. Es decir, que entre estas cinco hiperempresas (seguidas por Netflix) están centralizando las conexiones de 1300 millones de personas**[70]**.

Esa concentración de poder en pocas manos les da a las grandes compañías una tentación difícil de evitar: si por ellas pasa la información, el entretenimiento y el consumo del mundo, también son dueñas del enorme poder que implica controlar cantidades siderales de datos e información de las personas que confían en sus servicios. Allí está uno de los grandes conflictos de internet hoy: ¿cómo controlar o al menos regular ese enorme poder de las corporaciones de la Red?

Pero la centralización no solo fue una tentación para las empresas. Los gobiernos del mundo también cayeron en ella si los ciudadanos dejan allí sus rastros, ¿cómo evitar utilizarla para meterse en sus vidas? La mayoría de los Estados del mundo comenzaron no solo a recabar la información para perseguir a todo tipo de criminales, sino también para vigilar a cualquier persona, sospechosa o no. Al convertirse en una

forma cada vez más sencilla y barata de obtener información, ¿cómo evitar el abuso? Algunos países orientales, calificados de dictaduras por Occidente, como China o Irán, generaron mecanismos para transformar a la Red en un arma de control: construyen *firewalls* o barreras que filtran las comunicaciones para sus habitantes, utilizan el espionaje en internet para censurar, perseguir y hasta encarcelar disidentes y monitorean las comunicaciones de los opositores para generar un efecto de temor y disuadir las voces en contra de sus regímenes. Estos abusos suelen ser denunciados por gobiernos y organizaciones de derechos humanos de Occidente. Sin embargo, Estados Unidos y otras potencias capitalistas también se apoderaron de la Red y la utilizaron como un arma al servicio del espionaje y la vigilancia, solo que con una excusa con mejor *marketing*: la lucha contra el terrorismo y la defensa de la seguridad nacional.

Internet nació en la Guerra Fría, con el miedo a la bomba atómica a sus espaldas, y creció y se concentró en los años 90 de la globalización financiera. En 2001, con dos bombas en forma de aviones que atravesaron las Torres Gemelas de Nueva York, el terrorismo contribuyó a utilizarla como un arma contra el nuevo temor: el terrorismo. Los gobiernos del mundo la convirtieron en un gran artefacto de vigilancia global. Pero el abuso de ese poder también la hizo explotar.

Sin embargo, el siguiente estallido no fue espontáneo. Necesitó del movimiento de un grupo de personas que encendieron las mechas de otras bombas: los secretos de Estado. Entre ellos, el periodista y programador australianao Julian Assange fue el primero en volverse público, cuando a partir de 2010 convirtió a internet en un muro planetario de divulgación de confidencias ocultadas por el poder. El segundo fue Edward Snowden, un informático de entonces 29 años, que realizó su aparición en junio de 2013, cuando detonó su dinamita —en forma de un disco rígido lleno de archivos clasificados— y causó el mayor cambio en internet desde la Guerra Fría[71].

Con ellos comenzó una nueva era de internet, plagada de guerras que recién estamos comenzando a luchar.

V

Destruir secretos, una nueva forma de activismo

> «Edward Snowden nos ha recordado sencillamente a todos la extraordinaria capacidad de cualquier ser humano para cambiar el mundo».
>
> GLENN GREENWALD.
> *Snowden. Sin un lugar donde esconderse* (2014).

> «Solo tenemos los derechos que protegemos. No importa lo que digamos. No es suficiente con creer en algo. Lo que importa es lo que realmente defendemos».
>
> EDWARD SNOWDEN.
> *Citizenfour*[72].

El 11 de septiembre de 2001, cuando un atentado terrorista derrumbó las dos torres del Word Trade Center, Edward Snowden tenía 18 años. Con sus padres recién separados, el adolescente se había quedado con su madre y su hermana en Maryland, al noroeste de Estados Unidos. A pocos kilómetros de su casa, camino a Fort Meade, había un cartel que decía: «Acceso a Empleados. Agencia Nacional de Seguridad (NSA)». Snowden todavía no lo sabía pero esas tres letras significarían, diez años después, el punto de inflexión de su vida. Y el de la de todos los ciudadanos y usuarios de internet del planeta.

Edward Joseph Snowden había nacido en 1983 en Carolina del Norte, en la costa este de Estados Unidos, con el ejército, la tecnología y la justicia en su ADN. Su padre era oficial de la Guardia Costera de las Fuerzas Armadas, su madre se encargaba de mantener las computadoras de un tribunal de Baltimore y su hermana se convertiría en abogada del Tribunal Federal de Washington. Snowden fue un clásico hijo estimulado de los 80: era autodidacta de la computación, apasionado de los videojuegos, de los cómics manga y las artes marciales. Estaba fascinado con Japón y, con internet, se convirtió en un participante activo de los foros del sitio ArsTechnica, sobre computadoras, ciencia y tecnología.

Pero Snowden no era solo un *geek*. Tras los atentados a las Torres Gemelas, empezó a expresar su preocupación por la creciente pérdida de la privacidad de los estadounidenses. En 2002, bajo el seudónimo «The True Hooha» (el verdadero lío), le respondió a otro usuario de un foro que le cuestionó su insistencia por postear

diversas formas de ocultar su identidad: «Por el Acta Patriótica. Si interpretan mal mis actos, podrían tomarme por un ciberterrorista». Snowden se refería a la ley sancionada un mes después de los atentados del 11-S, que ampliaba la capacidad de vigilancia y endureció las penas para los delitos de terrorismo.

Sin embargo, Snowden no era un izquierdista ni un anarquista. Vivía en los Estados Unidos de los 2000, donde la guerra y el terrorismo ocupaban las noticias, y en 2004, a los 21 años, se unió al ejército. Su sueño era integrar las Fuerzas Especiales o Boinas Verdes, una unidad de elite. Pero no tuvo suerte: a poco de incorporarse, se rompió las piernas en un accidente durante un entrenamiento y lo mandaron a trabajar como guardia de seguridad en las instalaciones de la NSA en la Universidad de Maryland. Snowden estaba nuevamente cerca de su destino.

En 2006, empezó a trabajar en la CIA como experto en seguridad informática y en 2007 fue destinado a Ginebra, Suiza. Allí, Snowden ya tenía un acceso privilegiado a una amplia red de secretos del Estado, que podría haber revelado sin problemas. Pero esperó. Y se preparó. Unos años después, explicó que la mayoría de esos secretos implicaban a personas, no a sistemas, y que su verdadero objetivo era exponer la cara oculta de las actividades de la NSA, no a los ciudadanos. Durante esa espera se volvió un experto en penetrar bases de datos y documentos y comprendió de lleno cómo se libraban las guerras cibernéticas para espiar a otros países. En 2009, Snowden dejó la CIA. Trabajó para Dell en Japón, donde conoció a su novia, y en 2013 se mudó con ella a Hawai, donde se empleó en la empresa contratista de defensa Booz Allen Hamilton como administrador de sistemas, al servicio de la NSA. Vivía con su amor en una isla con palmeras y ganaba 20 mil dólares al mes, pero él tenía otro plan: terminar de copiar más de 20 000 documentos «Top Secret» de la NSA y darlos a conocer en junio.

Snowden necesitaba aliados. Pero no podían ser cualquiera, sino personas que pudieran ir más allá del escándalo y demostrar que los documentos eran parte de decisiones políticas que afectaban a los ciudadanos. Con ese objetivo, en 2012 había iniciado el contacto con dos periodistas de gran trayectoria en la investigación de violaciones a la privacidad y defensa de los derechos civiles: Glenn Greenwald, abogado y entonces columnista del diario inglés *The Guardian*, y Barton Gellman, periodista ganador del Pulitzer, de *The Washington Post*. Su tercer contacto clave lo realizó con la documentalista y activista Laura Poitras, multipremiada por una serie de tres películas que mostraban los abusos que había cometido Estados Unidos tras los atentados del 11 de septiembre, en Irak y en la cárcel de Guantánamo[73]. Tanto Poitras como Greenwald venían denunciando la vigilancia del Estado a sus ciudadanos y habían enfrentado por esto ataques de la prensa y de funcionarios. En 2013, ya en Hawai, Snowden los contactó nuevamente —todavía en forma anónima — para ofrecerles el material que había recolectado sobre un programa de espionaje llevado a cabo por la NSA. Sin una respuesta concreta de ellos, Snowden decidió que era tiempo de partir. Pidió una licencia médica y se subió a un avión con destino a

Hong Kong. Tenía dinero, cuatro computadoras y un lugar dentro de China que le garantizaba libertad de expresión y estar lejos del radar de los servicios secretos estadounidenses. Detrás, dejaba su vida cómoda a los 29 años, un buen sueldo, una novia y una casa con vista al mar. Por delante, todo era un misterio. Pero ya se había decidido. Ya había dado el gran salto.

Desde los atentados de 2001, con la amenaza de un nuevo golpe terrorista sobre sus hombros, Estados Unidos había convertido a todas sus agencias estatales de seguridad en una gran máquina de recopilación de información. Como mostró diez años después la serie *Person of Interest*[74], el país montó un sistema de vigilancia masiva que monitoreaba, recolectaba y analizaba datos de cámaras, comunicaciones electrónicas, audios e imágenes, con el fin de prevenir ataques en su territorio. En la ficción, el señor Finch, creador de La Máquina, describía su invento como «Diez mil ojos que todo lo ven y diez millones de oídos que todo lo escuchan. Algo que está en todas partes y en ninguna». Finch, una mezcla de científico y *hacker* con pasado misterioso, no ocultaba los objetivos de su invento: «El gobierno tiene un sistema secreto que te espía cada hora de cada día. Lo diseñé para detectar actos de terror, pero puede ver todo». El problema, tanto en la ficción como en la realidad, fue justamente ese: la monumental red de vigilancia creada por Estados Unidos podía monitorear todo. Y se hizo adicta a su propio poder: la acumulación de secretos.

Como ya había sucedido durante la Guerra Fría, el miedo llevaba a querer conocer cada detalle del enemigo, aunque todavía no fuera un rival. Pero mientras que en los 50 se necesitaban dispositivos de grabación más sofisticados y costosos, hoy la información estaba concentrada en un solo lugar: en las venas del monstruo de internet, en sus bases de datos y las comunicaciones digitales de cada usuario/ciudadano. Y no solo eso: al concentrarse la Red en unas pocas empresas que reunían bajo sus servicios, redes sociales y aplicaciones todas las transacciones de la vida de la gente, era mucho más fácil acceder a la información. Bastaba con contar con la cooperación de esas megaempresas (Google, Yahoo, Microsoft, las compañías operadoras de teléfonos celulares y proveedores de internet), para acceder al mayor núcleo de información del mundo.

Bajo el Acta Patriótica, las agencias de seguridad de Estados Unidos habían realizado un cambio en su sistema de recolección de datos que terminó volviéndoles como un boomerang mortal: consolidaron toda la información de los ciudadanos en una base de datos cada vez más centralizada, para que cada agencia involucrada en la lucha antiterrorista pudiera acceder a ella fácilmente. En el documental *We Steal Secrets, the story of WikiLeaks* (2013), Michael Hayden, director de la NSA entre 1999 y 2009, explica que, después del ataque contra las Torres Gemelas, su país no sabía cuál era exactamente su enemigo, con lo cual todos eran potenciales sospechosos. Entonces decidió comenzar a compartir la información entre sus

distintas agencias de seguridad y, al mismo tiempo, a guardar cada vez más información de sus ciudadanos y de extranjeros. «La cantidad de documentos secretos pasó de 8 a 76 millones. Los funcionarios con acceso a esa información llegaron a 4 millones. El gobierno interceptó llamadas y mensajes electrónicos de a 60 000 por segundo. Ni siquiera el Congreso sabía cuánto gastábamos del presupuesto para esta tarea». En el mismo documental, Bill Leonard, el Zar de los Documentos Clasificados de Estados Unidos entre 2002 y 2008, confiesa: «Generamos más secretos que los que producimos en toda nuestra historia».

La «era del miedo» es también la «era del secreto». Pero querer saberlo todo sobre cada ciudadano fue el talón de Aquiles de la gran maquinaria de recopilación de información: esa capacidad de vigilancia total también generaba la tentación de contarlo todo, no solo sus secretos, sino también sus abusos. Y, efectivamente, comenzaron a ser destapados. Durante varios años, las filtraciones se transformaron en titulares de los grandes medios del mundo. Paradójicamente, la era de las revelaciones florecía en los mismos años que mostrar todo se hacía lo normal en la web, con todos nosotros, celular en mano, dejando —voluntaria e involuntariamente — nuestra información y detalles cotidianos en las entrañas de la Red.

Sin embargo, los secretos —especialmente los de Estado— no salieron solos a la luz. Se necesitó, para destapar la compuerta, de la acción de un grupo de hombres cargados de armas técnicas y voluntad política. La explosión fue muy parecida a otra que había sucedido en los 70, cuando la figura de los informantes (o *whistleblowers*) había cobrado fama con dos escándalos políticos de magnitud: «Los papeles del Pentágono[75]» y luego con el «Watergate[76]». En ambos casos, la información había sido desenmascarada desde adentro del Estado por un «filtrador» y luego se había hecho pública al llegar a las tapas de los grandes medios gráficos.

Cuarenta años después, los informantes emergieron desde las profundidades de internet. Pertenecen a una generación que domina la tecnología para encontrar los secretos que se esconden en las grandes bases de datos. Al mismo tiempo, se trata de la generación que utiliza la Red, para distribuir lo oculto.

Lejos de obtener respaldo unánime en la sociedad, se acusó a los «delatores» de traidores y de quebrar la «gobernabilidad». El argumento es que si cada uno rompe las leyes porque no le gustan, el sistema político se volvería muy inestable. Pero, contra esta idea, también se puede argumentar lo contrario: ¿y si la traición es parte de la democracia? En el libro *Elogio de la traición*, los franceses Denis Jeambar y Ives Roucaute sostienen que «la traición es la expresión política de la flexibilidad, la adaptabilidad, el antidogmatismo», y que, a diferencia de la cobardía, es un mecanismo que «evita las rupturas y las fracturas», con lo que garantiza la continuidad de la democracia. En definitiva, se trata de sacar a luz las contradicciones. En el caso de los alertadores que se multiplicaron desde 2010, se unieron para demostrar que ese mismo sistema que decía proteger a sus ciudadanos de ataques terroristas —en pos de la seguridad—, se estaba inmiscuyendo tan

profundamente en sus vidas como para dañar otros derechos fundamentales: la libertad y la privacidad. Lo que venían a denunciar era que, en nombre de la democracia, el Estado se estaba transformando en una máquina tiránica controlada por unos pocos (gobierno y empresas privadas) que decidía a quién espiar y qué secretos guardar, sin dar cuenta de ello ante sus propios ciudadanos.

Entre aquellos que alzaron la voz contra el secreto hubo un líder que se hizo más visible y que allanó el camino para los que le siguieron. Mundialmente conocido antes de cumplir los 40 años, su nombre, Julian Assange, se convirtió en sinónimo de un nuevo artefacto —un sitio y una red de informantes— que se encargaría de desperdigar los secretos del poder alrededor del mundo: WikiLeaks.

Julian Paul Assange nació en Australia el 3 de julio de 1971. A los 16 años ya era un *hacker* con un talento reconocido por la comunidad. A los 20, cuando estudiaba física y matemáticas e integraba el grupo de hacktivistas «Subversivos Internacionales», la policía asaltó su casa de Melbourne y allí inauguró la larga saga de detenciones de su vida. En 1991, vía módem, ya había entrado a computadoras de universidades australianas y compañías de seguridad. En 1997 creó un paquete de programas para Linux destinado a ser, como diría más tarde, «una herramienta para trabajadores por los derechos humanos que necesitaban proteger información sensible, como listados de activistas y detalles sobre abusos cometidos».

La génesis de su idea de los individuos unidos, luchando contra las grandes instituciones, estaba ya presente en su manifiesto «La conspiración como forma de gobierno[77]», de 2006. Allí decía que el autoritarismo se construye cuando un grupo de poderosos actúa «bajo un secreto conspirativo, trabajando en detrimento de la población». En consecuencia, para Assange, el objetivo es destruir ese aparato. Y eso se logra cortando o interviniendo en las formas de comunicación de las autoridades para evitar que la maquinaria de la información secreta opere con tranquilidad. En otras palabras: luchar contra el autoritarismo es desarrollar estrategias para revelar lo que el poder quiere que no se sepa. En esa lucha, la tecnología se convertiría en un arma fundamental.

Ese mismo año, y para llevar adelante el objetivo expresado en su manifiesto, Julian Assange fundó y se convirtió en el editor en jefe de WikiLeaks. Desde entonces, el sitio se encarga de difundir informaciones de interés público, a través de una red de colaboradores repartidos por el mundo: periodistas, ingenieros, abogados, programadores y cualquiera que quiera aportar a la causa. Su consigna, que es también el primer y sagrado mandamiento de *La ética hacker*[78], es «poner en común la información». Pero no cualquier información, sino aquella que desenmascare intereses del poder. En palabras de Assange: «Trabajamos con una filosofía: las organizaciones que son abusivas tienen que estar en el ojo público».

Durante sus primeros años, WikiLeaks expuso una mezcla de secretos que incluían desde torturas en la cárcel norteamericana de Guantánamo en Cuba, hasta manuales confidenciales de la Iglesia de la Cienciología y listas de contribuyentes de campañas políticas. En 2008, la organización tuvo su año de verdadero impacto, cuando dio a conocer el «Asesinato colateral», un video donde dos soldados norteamericanos asesinaban a un periodista iraquí de la agencia de noticias Reuters, a su ayudante y a nueve personas más (entre ellas, niños), mientras tomaban una foto del helicóptero Apache donde viajaban los militares. Tras ese video, llegaron otras dos grandes revelaciones, en 2010, conocidas como «Los diarios de la guerra de Afganistán» y «Los documentos de la guerra de Irak». Allí se exponían públicamente más de doscientos mil archivos ultrasecretos de inteligencia que revelaban las víctimas civiles provocadas por el ejército de los Estados Unidos y sus aliados, y las conexiones con la inteligencia paquistaní y con los talibanes insurgentes. Luego de conocerse esas informaciones, Bradley Manning, un soldado norteamericano apostado en Bagdad, fue arrestado y confinado a una reclusión absoluta, acusado de haber filtrado los documentos a WikiLeaks[79].

WikiLeaks se asoció en la primera etapa de sus revelaciones con *The Guardian, The New York Times* y *Der Spiegel*, tres de los diarios más importantes de Estados Unidos y Europa, para lograr un impacto mayor en la opinión pública internacional. La «prensa tradicional» fue, en ese momento, aliada estratégica de la nueva forma de contrainformación. Ese mismo año, la organización liderada por Julian Assange dio su otro gran golpe, conocido como «Cablegate», al filtrar a la prensa internacional doscientos cincuenta mil cables entre el Departamento de Estado estadounidense con sus embajadas por todo el mundo. El impacto fue aún más grande, ya que en cada país involucrado con los cables diplomáticos la prensa local investigó y publicó las historias que relacionaban a sus cúpulas políticas o empresarias con el Departamento de Estado norteamericano (su ministerio de Relaciones Exteriores). Como señaló el periodista británico Christopher Hitchens, «la sagacidad de la estrategia de Assange consiste en que ha hecho a todos cómplices en su propia y privada decisión de sabotear la política exterior norteamericana». Al finalizar ese 2010, el líder de WikiLeaks se había convertido, según la revista *Time*, en «el hombre más peligroso de Estados Unidos». Para los gobiernos de todo el mundo, también se había transformado en la amenaza más temida.

El 7 de diciembre de 2010, Assange fue nuevamente arrestado. El motivo fue una causa iniciada seis meses antes en Suecia, cuando dos mujeres lo acusaron de forzarlas a tener relaciones sexuales sin protección, un acto considerado ilegal en ese país. Assange y sus defensores sostienen que el *affaire* fue una operación armada desde Estados Unidos. Su abogado inglés, Mark Stephens, declaró que su cliente fue sometido a una trampa de «fuerzas oscuras». Enemigos no le faltaban en su trayectoria como activista. En los hechos judiciales, la denuncia por acoso sexual había sido desestimada anteriormente, pero cuando explotó el Cablegate el país

nórdico emitió una orden de captura internacional y Assange, que estaba viviendo en Londres, se presentó voluntariamente a la justicia y quedó en manos de Interpol. Como cuando tenía 20, el australiano salió libre bajo fianza. Pudiendo volver a Suecia, Assange y sus abogados decidieron que viajara a ese país, temiendo que sus autoridades facilitaran su extradición a Estados Unidos, un país donde no iba a ser bien recibido, por razones obvias. Pero finalmente decidió quedarse en Londres, aceptando el ofrecimiento de asilo del presidente de Ecuador, Rafael Correa, para permanecer en su sede diplomática en la capital inglesa. Allí, el fundador de WikiLeaks vive desde el 19 de junio de 2012, en una habitación de doscientos metros cuadrados, donde combina su vida y su trabajo. No usa *email* y se comunica con sus colaboradores preferentemente en persona. «Tengo que actuar como Osama bin Laden ahora», escribió en su libro *Cuando Google conoció a WikiLeaks*.

Tal como se lo propuso Assange en su manifiesto, las revelaciones de WikiLeaks implicaron una gran «pérdida de control» para Estados Unidos, sus agencias de seguridad y militares, y sus corporaciones económicas. Assange se convirtió, para el Gobierno, en una especie de terrorista que les proponía un juego de escondites que ellos mismos, acostumbrados a lidiar con el secreto, no podían manejar. Pero no solo eso: ante cada ataque a su persona o a WikiLeaks, Assange contaba con un ejército de ciberguerreros y de hacktivistas que aparecían desde todos los puntos de la Red en el mundo para apoyarlo. Cada afrenta contra él era como tirar miel en un campo minado de abejas: todos se unían para defender la causa. Entre los más conocidos estaba Anonymous, un grupo de hacktivistas que había comenzado a forjar su identidad unos años antes y que tuvo una de sus mayores actuaciones en 2012 con la Operación Payback. Su objetivo fue vengar los bloqueos financieros que Visa, MasterCard, PayPal y Amazon le habían impuesto a WikiLeaks con el fin de que no llegaran donaciones al sitio, justo después de la revelación de miles de cables diplomáticos y la persecución de su líder Julian Assange. En venganza, Anonymous inhabilitó los sitios de las tarjetas de crédito durante un día entero.

Si bien la atención se centró en él, Assange no fue el primer periodista, *hacker* y activista decidido a revelar secretos militares por la libertad de la información. «Sería un error enfocarse solamente en cómo WikiLeaks ha sido castigado y saboteado mientras ignoramos una lección más amplia: cómo el grupo inspiró una generación entera de *hackers* políticos y reveladores de secretos digitales. La historia no comenzó ni terminó con Julian Assange, ni con su grupo. Al contrario, lo que hace es recorrer los ideales, los medios y el movimiento que WikiLeaks representa, que se extiende desde sus predecesores, décadas antes, hasta sus seguidores ideológicos, que se han movilizado radicalmente», dice Andy Greenberg[80], periodista de la revista *Wired* que escribió la primera nota de tapa sobre Assange en esa publicación.

Sin embargo, Assange tuvo un mayor impacto porque, como dice el filósofo esloveno Slavoj Žižek, el líder de WikiLeaks espió «para el pueblo», es decir, socavó el principio mismo del secreto al hacerlo público y decirnos lo que tenemos en frente

nuestro pero no podemos verlo, sumergidos en la fantasía de la democracia. Si antes las revelaciones se hacían ante un Estado para pedirle protección, Assange apuntó directamente al Estado y le dijo a la gente algo que todos sabíamos pero no asumíamos como verdadero: que nos espían sin avisarnos o que nos mienten sobre una guerra. Según Žižek[81], la importancia de Assange consistió en mostrar los detalles: «Es un poco como enterarse de un engaño amoroso: puede ser aceptable el conocimiento abstracto de la situación, pero el dolor emerge cuando se revelan los detalles ardientes, cuando se consiguen imágenes explícitas de lo acontecido». Al mostrar lo oculto, dice el filósofo, WikiLeaks hace algo más valioso que decir que hay un régimen opresivo: nos dice que esa falta de libertad existe en un mundo que creemos libre. Nos dice que el país donde vivimos, al cual no le encontrábamos un problema aparente, sí tiene problemas. Nos dice que dejemos de mirar hacia los regímenes dictatoriales como China o Rusia (que ciertamente son autoritarios) y nos enfoquemos un momento en nosotros mismos: ¿cuán libres somos, realmente?

Assange, desde la embajada de Ecuador en Londres, se había convertido en un vocero, no solo de la censura y la vigilancia en internet, sino en un denunciante de todo tipo de poderes concentrados, desde los medios de comunicación hasta el sistema financiero internacional. También, puso en la portada del debate público el rol de la tecnología usada para controlar a los ciudadanos y la colaboración de las corporaciones para este fin. En octubre de 2014 publicó *Cuando Google encontró a Wikileaks*, un libro donde revelaba una conversación que había mantenido en 2011 con Eric Schmidt, el CEO de la empresa. Assange le dijo al mundo que «las empresas como Google y Facebook están en el mismo negocio que la Agencia de Seguridad Nacional de Estados Unidos» cuando recolectan enormes cantidades de información de todos nosotros la integran y la utilizan, unos con fines comerciales (las empresas de internet) y otros con fines de control de los ciudadanos (los gobiernos). Assange advertía: estamos inmersos en una guerra que lucha entre lo democrático y lo autoritario, y donde no hay buenos y malos fácilmente distinguibles, sino algo más complejo: los grandes poderes cooperan entre sí. Por lo tanto, si los ciudadanos no tomamos las armas para defendernos, eso seguirá pasando.

Desde su asilo siguió comandando su organización, revelando secretos y dando notas a medios del planeta. Cuando, después de sus revelaciones, Snowden tuvo que escapar de Hong Kong, ya sin el apoyo de los medios que lo habían ayudado a difundir sus secretos, Julian Assange y su organización fueron su gran apoyo. «Fue la persecución de inteligencia más grande de la historia de la humanidad —dijo Assange—. Yo estaba en medio de una publicación, tenía temas judiciales en seis jurisdicciones y estaba en el medio de una campaña electoral. Dejamos todo y nos pusimos a trabajar. Invertimos muchos recursos y pagamos un precio muy alto[82]».

El 20 de mayo de 2013 Edward Snowden llegó al aeropuerto de Hong Kong con sus computadoras llenas de secretos, los ojos resguardados en sus antejos rectangulares y la cabeza tapada por una capucha. Retomó el contacto con Glenn Greenwald y le preguntó si ya había instalado herramientas básicas de seguridad para enviarle una muestra de la información secreta. Snowden no podía arriesgarse a confiarle ningún material si el periodista instalaba, al menos, el programa PGP (PrettyGoodPrivacy), un *software* que encripta los mensajes y los protege de la vigilancia. Como recordaría más tarde Greenwald en su apasionante libro *Snowden. Sin un lugar donde esconderse*: «Hacía tiempo que quería usar *software* de encriptación. Llevaba años escribiendo sobre WikiLeaks, los delatores de ilegalidades, sobre Anonymous y también había establecido comunicación con personas del *establishment* de seguridad nacional de Estados Unidos. Por todo ello, el uso del *software* de codificación era algo que tenía en mente. Sin embargo, el programa es complicado, sobre todo para alguien como yo, poco ducho en programación y computadoras. Era una de esas cosas para las que nunca encuentras el momento». Entonces Snowden le envió un video subido a YouTube con una guía detallada, bajo el título «Encriptación para bobos».

Mientras tanto, Snowden había comenzado a mandarle materiales secretos a Laura Poitras, que ya había trabajado con documentos confidenciales. Cuando recibió la información, la documentalista supo al instante que se trataba de una revelación que cambiaría su vida y la del mundo. Lo llamó a Greenwald, que voló de inmediato desde su casa en Río de Janeiro a Nueva York, y lo citó en un bar bajo una condición: no llevar su teléfono celular. Poitras ya sabía que los móviles eran la herramienta perfecta para que los servicios secretos escucharan su conversación. No bastaba con quitarle la batería. Lo que estaba pasando era tan importante que solo podía decírselo en persona. Tras la reunión, Greenwald también entendió que debían viajar inmediatamente a Hong Kong. Lo de Snowden (aunque todavía no conocían su verdadera identidad) parecía a todas luces verdadero. El periodista aprendió finalmente a cifrar sus comunicaciones, habló con su diario, *The Guardian*, para que financiaran su viaje y el 1.º de junio de 2013 partió con Poitras a Hong Kong. En el avión, leyó el primer documento: en él, el Tribunal de Vigilancia de la Inteligencia Extranjera de Estados Unidos le solicitaba a la empresa de telecomunicaciones Verizon que transmitiera los registros telefónicos de sus clientes al gobierno. La empresa entonces tenía 13 millones de usuarios en el país. La vigilancia era masiva y ese era solo uno de los miles de documentos. Pero lo más importante de todo: tenían las pruebas. Las sospechas sobre las que periodistas, políticos y organizaciones de derechos humanos habían denunciado y pedido información al gobierno finalmente eran ciertas. Estaban allí. Solo faltaba hacerlas públicas.

El encuentro de Greenwald y Poitras con Snowden fue tan cinematográfico como una película de James Bond en la era de internet. «La cita se había fijado a la manera clásica de los agentes secretos: en el barrio Kowloon, delante de un restaurante, donde deberían identificarlo gracias al Cubo de Rubik que tendría en la mano. Entonces deberían preguntarle: "¿A qué hora abre este restaurante?". Si el hombre respondía la hora y agregaba que el restaurante era malo, se trataba de su interlocutor[83]».

Los periodistas se sorprendieron ante la juventud de Snowden, pero lo acompañaron al interior de una habitación del lujoso hotel Mira. Cubrieron la puerta con almohadas para aislar las conversaciones y colocaron sus celulares dentro de la heladera del minibar. A esa altura, todos sabían por qué: la técnica creaba un efecto llamado «jaula de Faraday», que bloquea la señal de radio e impide que transmita datos a los servicios secretos. Poitras encendió su cámara y Glenn Greenwald entrevistó a Snowden durante cinco horas. «Quería estar seguro de la coherencia de sus afirmaciones», escribió el periodista. Pero tras la conversación, ya no tuvo dudas. Durante varios días trabajó sin dormir en una serie de notas que publicaría en *The Guardian*.

El 5 de junio de 2013, cuatro días después de llegar a Hong Kong, el diario británico difundió la primera exclusiva: «La NSA recolecta cada día los registros telefónicos de millones de abonados a Verizon[84]». Al día siguiente, Laura Poitras y Barton Gellman continuaron en *The Washington Post*[85] con una historia todavía más impactante, porque involucraba a casi todos los usuarios de internet del mundo «La NSA y el FBI interceptan información de nueve de las principales empresas estadounidenses de internet, directamente de sus servidores centrales, de donde extraen los chats de audio y video, las fotografías, los correos electrónicos, los documentos y los identificadores de conexión, lo que les permite a los analistas llegar hasta blancos extranjeros». El megasistema de espionaje se llamaba Prism, realizaba 2000 informes mensuales de vigilancia y gastaba anualmente 20 millones de dólares. Las empresas involucradas no eran una parte menor del escándalo, ya que se trataba de casi todas las que utilizamos cada día para nuestra comunicación *online*: Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube y Apple. Tras las revelaciones, todas ellas desmintieron la existencia de su relación con el programa de espionaje. Google comunicó: «Nosotros solo divulgamos datos al Gobierno Federal de acuerdo con la ley y examinamos cuidadosamente cada petición». Facebook realizó una declaración similar y Apple señaló: «Nosotros no proveemos ningún acceso directo a nuestros servidores a ninguna agencia gubernamental y toda agencia de este tipo que solicite datos sobre un cliente debe obtener una orden judicial».

La respuesta del gobierno de Barack Obama también llegó al día siguiente: «Nadie está escuchando conversaciones telefónicas de la gente». Pero luego relativizó la declaración diciendo que era necesario «balancear» la protección de la vida privada y la lucha antiterrorista. «En términos abstractos, la gente puede

quejarse de que esto es el Gran Hermano y de que este programa se nos ha ido de las manos. Pero cuando se miran los detalles, creo que hemos alcanzado el equilibrio correcto», dijo. Sin embargo, quizá el punto más escandaloso fue una aclaración sobre Prism: «No se aplica a ciudadanos de Estados Unidos». El Presidente de la máxima potencia del mundo estaba, con esas palabras, admitiendo que su aparato tecnológico de vigilancia estatal sí trabajaba para espiar las comunicaciones telefónicas y *mails* de ciudadanos extranjeros.

Al día siguiente, el escándalo siguió adquiriendo magnitud. *The Guardian* publicó *online* un video de 12 minutos que revelaba la identidad del delator de los secretos. En él, Edward Snowden, filmado por Poitras y entrevistado por Greenwald en Hong Kong, de espaldas a un espejo, con una camisa gris, su tono calmado y seguro, sus ojos marrones detrás de los marcos de los anteojos, decía: «Me llamo Ed Snowden, tengo veintinueve años, trabajé para Booz Allen Hamilton como analista de infraestructura para la NSA en Hawai. Soy como todo el mundo, no tengo ningún talento particular. Soy un tipo más que va a la oficina todos los días, que mira lo que pasa y piensa: “No nos corresponde a nosotros decidir sobre esto, es el público el que necesita decidir si estos programas y esta política son correctos o incorrectos[86]”». En él, también agregaba el sentido que había impulsado su acto de valentía: «Me niego a vivir en un mundo en el que cada cosa que digo, cada cosa que hago, es grabada, en un mundo en el que no hay privacidad, por lo que no hay espacio para el pensamiento libre».

Ese día de junio y los que siguieron fueron frenéticos para los periodistas, y más todavía para los que escribíamos sobre las consecuencias políticas y sociales de la tecnología. Recuerdo *mails*, mensajes y llamados de los editores de los medios para donde escribo, de otros colegas que cubren otros temas y a veces me consultan sobre cuestiones de tecnología, y hasta de amigos y familiares. El comentario era el mismo: «Al final, no era exagerado lo que decías sobre cómo internet se usa para vigilar a la gente». Snowden había confirmado el miedo, había mostrado las pruebas de lo que imaginábamos como real. Ellas eran tan concretas como unos archivos de Power Point horriblemente diseñados —«la NSA necesita un diseñador» fue un chiste común en aquellos días— donde se mostraba cómo a través del programa Prism el gobierno norteamericano trabajaba en colaboración con las empresas de tecnología para espiar a la gente.

Lo que venía escribiendo como periodista, lo que antes había denunciado Assange y otros tantos activistas por los derechos en internet, ahora estaba allí para que todos lo vieran. Esa era la mejor noticia. Porque transformaba en tangible algo que por momentos era difícil de explicar: en internet, con las herramientas adecuadas y la colaboración de quienes controlan nuestra información, se puede ver todo lo que hacemos. La única forma de que eso no pase es que nosotros lo impidamos, evitando usar productos de las compañías que colaboran con el espionaje, encriptando nuestras

comunicaciones y manteniendo el control de lo que decimos, publicamos o subimos a la Red. Ya no se trataba de paranoia. Era real.

Después de conocerse su identidad y el video, Snowden se fue del territorio chino y durante algunas semanas nadie supo de él. Tras varios pedidos de asilo político (entre ellos al presidente Rafael Correa de Ecuador, que ya había ayudado a Julian Assange) y cruces diplomáticos por su destino (por ejemplo, la demora del avión del presidente boliviano Evo Morales desde Moscú, con la sospecha de que allí se escondía Snowden rumbo a América Latina), el informático encontró asilo político en Moscú, donde permanece desde agosto de 2013.

En cuanto se supo la identidad de Snowden, la pregunta era qué lo había motivado a tomar el riesgo de enfrentarse a los grandes poderes. Para Glenn Greenwald en su libro, había un factor generacional y cultural en la decisión de Snowden: tenía que ver con una identidad moral construida en su vínculo con los videojuegos. «La lección aprendida por Snowden de su inmersión en los videojuegos era que una persona sola, incluso la menos poderosa, puede enfrentarse a una gran injusticia. El protagonista suele ser alguien que se ve frente a graves injusticias causadas por fuerzas poderosas y tiene la opción de huir asustado o luchar por sus creencias. Y la historia también pone de manifiesto que personas aparentemente normales con la suficiente firmeza pueden triunfar ante los adversarios más temibles».

Según el periodista, había otro rasgo generacional en la decisión de Snowden: su visión del mundo se había construido mientras también nacía y crecía la Red: «Como para muchos de su generación, para él internet no era una herramienta aislada para tareas concretas, sino el mundo en el que se desarrollaba su mente y su personalidad, un lugar en sí mismo que ofrecía libertad, exploración y el potencial para el conocimiento y el crecimiento intelectual», escribió Greenwald. Snowden se lo había dicho así: «Más que nada, internet me permitió experimentar libertad e investigar mi capacidad plena como ser humano. Para muchos niños, internet es un medio de autorrealización. Les permite explorar quiénes son y qué quieren ser, pero esto solo funciona si somos capaces de conservar la privacidad y el anonimato, de cometer errores sin que nos vigilen. Me preocupa que mi generación sea la última en disfrutar de esta libertad[87]».

A Snowden lo desvelaba eso: que su esfuerzo quedara como una noticia más de la lista de las más leídas del día y luego se perdiera, sepultada en otras novedades. Un año más tarde, en una entrevista en la revista *Wired*[88], lo decía así: «Es la banalidad del mal. Es como la historia de la rana que se quema de a poco, que no va sintiendo que se muere. Te exponés a un poco de mal, a un poco de leyes que se rompen, a un poco de deshonestidad, a un poco de engaño, a un poco de daño al interés público y podés ignorarlo un poco o justificarlo. Pero si lo hacés, se crea un terreno resbaloso

que crece y con el tiempo nada te impacta. Ves todo como normal». Greenwald lo había advertido: «Permitir a la vigilancia arraigar en internet significaría someter prácticamente todas las formas de interacción humana, la planificación e incluso el pensamiento a un control estatal exhaustivo». Recordando el origen abierto de internet, amenazado por su uso en manos concentradas bajo procedimientos ilegales, decía: «Convertir internet en un sistema de vigilancia destruye su potencial básico. Peor aún, transforma a la red en un instrumento de represión, lo cual amenaza con crear el arma más extrema y opresora de la intrusión estatal que haya visto la historia humana».

En octubre de 2014, Laura Poitras estrenó *Citizenfour*, el documental basado en las entrevistas que le había realizado a Edward Snowden en Hong Kong. En una de sus escenas más conmovedoras —tal vez aún más para los que hoy tenemos 30 y podemos identificarnos generacionalmente con él, con haber vivido una internet mucho más libre—, Snowden dice: «Recuerdo cómo era internet antes de estar siendo observado. Nunca hubo nada así. Digo: podías tener dos chicos en una punta y otra del mundo teniendo una discusión igualitaria, donde estaba casi garantizado el mismo respeto por sus ideas y su conversación, con expertos de un tema en una parte y otra del mundo, sobre cualquier cuestión, en cualquier lado, en cualquier momento. Y era libre y sin restricciones».

Pero la «bomba Snowden» ya había caído y las consecuencias fueron tan grandes que afectaron internet tal como la conocíamos. En todo el mundo, los presidentes de las potencias espiadas, entre ellos Angela Merkel de Alemania y Dilma Rousseff en Brasil, advirtieron que el espionaje de Estados Unidos a través de la NSA era inadmisible. Los cables diplomáticos revelados primero por Julian Assange y WikiLeaks en 2010, y ahora las escuchas y monitoreo intensivo de las comunicaciones convertían la tecnología aplicada al espionaje en algo insostenible.

El escándalo no afectó solamente a Estados Unidos. En cada país, el dilema también existía: ¿cómo manejar una información cada vez más concentrada?, ¿cómo dirimir la necesidad de seguridad ciudadana —una demanda genuina— con la privacidad —y la libertad—?, ¿cómo controlar a las agencias y las empresas para que no cometan abusos contra los usuarios-habitantes? Y, de ser así, ¿quién sería el responsable de ejercer ese control?

El coraje de Snowden fue tan contagioso que logró que esos debates se hicieran más públicos. «Hace poco, alguien dijo que las revelaciones sobre la vigilancia masiva de la NSA fueron el momento atómico de los informáticos. La bomba atómica fue el momento moral de los físicos. El espionaje masivo es ese mismo momento para los científicos informáticos: cuando se dan cuenta de que las cosas que producen pueden usarse para dañar a una cantidad tremenda de gente[89]», decía Snowden desde Rusia. Su acto tuvo la potencia de que volvieran a ser escuchadas las discusiones que venían planteando activistas de internet, periodistas y académicos del

mundo: ¿cómo hacer para que internet no se convierta en un arma contra las personas?

Snowden fue el responsable de acelerar esos debates en todo el mundo. Pero también cuestionó, por primera vez, el rol de Estados Unidos en el control de internet. Las propias organizaciones y la estructura de decisiones de la Red se vieron afectadas. Tras sus revelaciones la geopolítica de internet sufrió un terremoto cuyas réplicas se multiplicaron durante los meses y años siguientes. Como esos secretos que estallan un día en una familia y dividen las aguas, las consecuencias del acto de Edward Snowden fueron tan grandes que internet cambió para siempre.

Snowden, junto con Assange, plantearon, cada uno desde su lugar, que internet, además de suponer una época de gran movilización política y denuncias de opresión a través de nuevas herramientas de comunicación, es también una era de guerras que involucran nuestros derechos, especialmente la libertad y la privacidad.

Ambos, cada uno con sus bombas cargadas de información, unieron su voluntad común por romper con el secreto. Con eso, arremetieron contra algo fundamental: la ignorancia sobre cómo la tecnología está enmarañada en cada proceso de nuestras vidas. Si mantenemos ese desconocimiento, nuestra vida seguirá igual: confiando ciegamente en otros para que manejen nuestra vida digital. Pero ellos hicieron lo contrario. Al explotar la información que otros ocultaban, dejaron al descubierto que esos procesos no son del todo transparentes, sino que son manejados por personas, grupos de intereses y corporaciones.

Al abrir los secretos, Snowden, Assange, Greenwald y miles de activistas por los derechos de internet en el mundo logran generar un debate público sobre un tema que otros prefieren callar obligan a todos a debatir. No solo a los hacktivistas y los militantes más radicales sino a funcionarios, diplomáticos, corporaciones que tienen que salir a defender sus actos, y legisladores y hasta presidentes que se ven conminados a ocuparse de algunas cuestiones que antes eran solo territorio de ingenieros o expertos informáticos. Pero cuando los secretos son puestos a la luz, ya están allí y no es posible seguir evitándolos. Las peleas ya no son imaginarias o algo por venir. Se hacen reales. Y se luchan en cada escenario del mundo.

TERCERA PARTE

De Silicon Valley a Net Mundial: Cómo se cocina internet.

VI

Dilma contraataca: San Pablo, capital de la internet soberana

> «El ser humano no es mejor ni peor que hace miles de años. Egoísta en su esencia, todo su poder sobre este mundo lo ha obtenido, sin embargo, de la colaboración con los demás».
>
> ANA MARÍA SHUA.

—Somos un equipo. Tenemos que pensar un plan y ejecutarlo con coraje. El coraje es contagioso.

Las palabras de Jake Appelbaum son sagradas. Cuando él habla, el resto de los *hackers* y activistas lo escuchan con la atención de líder en una reunión improvisada entre escritorios y escaleras en el Centro Cultural San Pablo. Son las 4 de la tarde del 22 de abril de 2014. Esta noche, en el lujoso hotel Hyatt de Morumbí, al otro lado de la ciudad, se inaugura oficialmente Net Mundial, un gran encuentro que reunirá a gobiernos, organismos y activistas de todo el planeta para discutir el futuro de internet. Serán dos días de debate de la alta diplomacia de la Red para barajar nuevas cartas y trazar el plan de los próximos años, luego del tsunami generado por las revelaciones de Edward Snowden en 2013.

Pero esta tarde, bajando de la estación de subte Vergueiro, en el centro de la metrópolis, se gesta una operación secreta. Sus mentores somos quienes hoy nos reunimos en Arena Net Mundial, un encuentro de activistas, *hackers* y organizaciones de derechos de internet paralelo al gran evento. Nuestro objetivo es que la inauguración de la gran cumbre de la Red no pase desapercibida. Que el mundo se entere de que internet está en guerra.

Appelbaum, de 31 años, tiene la palabra. Con un libro en la mano, remera rayada y *jean* ajustado, anteojos de marcos negros gruesos, Jake es un *nerd* de trazos perfectos. Su mirada está atenta a cada movimiento del lugar y sus ojeras delatan que hoy durmió poco, pero su energía lo contradice. Frente al grupo de veinte personas a su alrededor, Jake habla en un inglés claro y pausado, algo afectado por el alemán de su hogar actual, Berlín. Le pide a un fotógrafo que evite tomar imágenes mientras discutimos y nos recuerda nuestro enemigo de mañana:

—Nuestro objetivo es Carl Bildt, el ex Primer Ministro de Suecia, que estará en la sesión de apertura de Net Mundial. Después de conocer que la NSA nos espía a todos,

el tipo dijo ¡que la vigilancia masiva es necesaria! ¿Lo vamos a dejar hablar sin decir nada?

Jake sabe de qué se trata ser vigilado. El 29 de julio de 2010 fue detenido durante tres horas en una sala de interrogatorios en el aeropuerto de Newark, Nueva York, para saber si él, un miembro reconocido de WikiLeaks en Estados Unidos, conocía el lugar donde estaba escondido su amigo Julian Assange. En el momento de mayor tensión en la vida de la organización: Assange había sido declarado «el hombre más peligroso de Estados Unidos» y Appelbaum era uno de los pocos hombres en quien el líder de la organización confiaba. Días antes del interrogatorio, Jake había hablado en nombre de Assange en la conferencia *Hackers of Planet Earth*. El australiano había elegido a Appelbaum como uno de los *criptopunks* de su círculo íntimo. El californiano, de entonces 27 años, ya tenía varias vidas extra viviendo como *hacker* y una contribución fundamental en el desarrollo de Tor, un navegador que protege la privacidad, usado por la mayoría de los hacktivistas del mundo.

Jake[90] viaja por el mundo como uno de los hacktivistas más reconocidos y el que toma la palabra en público en representación de compañeros de lucha como Assange y Snowden. En 2013, cuando Transparencia Internacional le entregó el «Premio Informante» al exconsultor informático de la NSA, Jake subió al escenario y habló por él. Ese día, Appelbaum también dijo: «El coraje es contagioso», comparando la valentía de Snowden con la de Daniel Ellsberg, quien reveló en 1971 «Los papeles del Pentágono». Hoy el destino de Jake es San Pablo. Pero el mensaje siempre es el mismo: contagiarse del coraje que tuvo Snowden. Por él, dice, hoy estamos en este lugar.

Estamos en Brasil donde la presidenta Dilma Rousseff convocó al resto de los países y los actores involucrados en el manejo de internet a discutir cómo estamos usando la Red y cómo la queremos usar en el futuro. Estamos para debatir, durante dos días, cómo lidiar con un invento que puede transformarse en un arma: de construcción y de libertad, o de destrucción y vigilancia. Pero, sobre todo, estamos en un punto de quiebre de la historia de internet: aquel que sigue después de las revelaciones de WikiLeaks y de Edward Snowden, que mostraron con hechos y documentos oficiales que la Red también puede usarse con la intención de espiar ciudadanos, perseguir disidentes y esconder secretos de Estados. Es un punto de no retorno: internet ya no permite miradas ingenuas, excepto que decidamos ignorar todas las advertencias, incluidas las palabras del propio Assange: «Internet, nuestro mayor instrumento de emancipación, ha sido transformado en la más peligrosa herramienta de totalitarismo que hayamos visto. Internet es una amenaza a la civilización humana[91]».

Por eso, mientras discutimos qué funcionario será mañana el objetivo de la protesta, la imagen a llevar en alto no admite discusión: es la de Snowden. Cada integrante del grupo de protesta improvisado tiene una pila de máscaras de él en la mano. Cada una consiste en una fotocopia con su cara, en hojas A4 blanco y negro,

con líneas punteadas para recortar a su alrededor, dos ojos para perforar y dejar la vista atenta, y dos círculos pequeños cerca de las orejas para atar una cuerda de lado a lado y sujetarla a la cabeza. La consigna es guardar las máscaras en la mochila, mezcladas con otros papeles y hacerlas pasar desapercibidas por los escáneres del hotel y las miradas de las fuerzas de seguridad.

—¿Quién tiene acreditación para entrar mañana al Hyatt con las máscaras y nos puede ayudar? —pregunta Jake—. A nosotros ya nos conocen y nos van a revisar todo.

Levanto la vista de mi libreta roja, alzo la mano y respondo rápido, como si fuera parte del grupo desde siempre:

—Yo me ofrezco. Soy periodista, soy argentina, estoy acreditada y todavía no hice nada demasiado peligroso. Voy a pasar sin problemas las máscaras.

El grupo me devuelve una sonrisa masiva y agradecida. «*Great*», me dice Jake. «*Thank you*», suelta una activista india. Algunos me dan la mano, otros me abrazan y una chica brasilera, la encargada de preparar la operación, me pregunta si tengo una mochila para llevarme ahora la pila más grande de fotocopias con la cara de Snowden. Estoy recién llegada a San Pablo, una ciudad de donde salís a la mañana sin saber a qué hora volvés. La mochila está llena de cosas: un desodorante, un mapa enorme, dos grabadores, una cámara, una camisa de *jean* contra el aire acondicionado del subte, unos zapatos formales que me cambio cuando necesito mejorar mi aspecto de periodista y entrar al Hyatt.

—Sí, algo de lugar me queda.

«¡*Legal*!», me dice la activista local, y me da las máscaras. Hago lugar en la mochila y las guardo adentro de una bolsa de supermercado que me quedó del almuerzo. Desde ahora y hasta mañana no me puedo despegar de ellas. Tengo una misión: llevarlas a la ceremonia de inauguración y repartirlas entre los activistas. Ahora yo también formo parte del plan, que continúa organizándose:

—Cuando Carl Bildt suba al escenario, nos ponemos de pie con las máscaras de Snowden y le gritamos que la vigilancia masiva no es necesaria, ni justa, ni legal. En Europa, este tipo fue uno de los voceros que la justificó diciendo que si hay terrorismo hay que espiar a todos, por las dudas.

Jérémmie Zimmermann toma la palabra. Es el único francés y uno de los pocos europeos en un círculo de norteamericanos, latinoamericanos e indios. Barbudo, de rulos largos sin peinar, los ojos pequeños de miopía detrás de los anteojos y una remera de *trollfaces*[92], Zimmermann está de viaje desde hace varias semanas, cuando inició un recorrido por América Latina. Como Appelbaum, su vida es viajar, tomar la palabra y crear acciones que contagien a activistas para defender la Red y sumarse al movimiento *criptopunk*[93], cuyo objetivo es encriptar todas las comunicaciones del mundo para que no puedan ser rastreadas por ningún gobierno o empresa. Jérémmie[94], fundador de La Quadrature du Net, una influyente organización europea por los derechos de la Red, es otro integrante del pequeñísimo

círculo de confianza de Julian Assange y una pieza fundamental del movimiento hacktivista actual[95]. Y hoy también está en San Pablo.

—Mañana el Hyatt va a estar lleno de cámaras. Tenemos que gritar «Gracias, señor Snowden, porque ahora vemos con claridad la gravedad del espionaje masivo». Tenemos que advertirle a los funcionarios del mundo que no nos vamos a pasar dos días hablando de internet ingenuamente mientras los gobiernos de muchos países usan la Red en contra de la gente, con la excusa de defendernos del terrorismo.

El grupo asiente. En las rampas y las escaleras sobre nuestras cabezas, grupitos de *skaters* paulistas nos pasan por encima a toda velocidad. El lugar está repleto, pero hay un silencio de acción.

—No podemos ir contra Dilma. Ella fue otra víctima del espionaje, aunque su gobierno también espió a otros. Pero no queremos ir contra Brasil.

Jérémmie cierra el debate. El grupo está de acuerdo. La votación dice que la protesta será contra Carl Bildt. Una integrante de la Electronic Frontier Foundation[96] de Estados Unidos propone que, además de las máscaras, hay que hacer algo más escandaloso, para que la prensa lo muestre. Sugiere llevar una torta de crema y aplastarla contra la cara y el traje —seguramente caro— del exministro sueco. La foto, dice, daría la vuelta al mundo. Pero Mishi Choudhary, una activista del *Software* Freedom Law Center de la India le advierte que ella está alojada en el Hyatt y que hay tanta seguridad que sería imposible entrar con una torta sin pasar por un interrogatorio. ¿Aerosoles de crema para decorar tortas, entonces? Menos todavía: los tubos de aerosol serían imposibles por la seguridad.

—Entonces hay que garantizar que la foto de las máscaras circule en todos los medios. Tenemos que asegurarnos de que eso suceda —dice Jake.

—Después de entrar con los carteles, yo voy a estar en el área de periodistas. Puedo sacar una foto cuando alcen las máscaras, por si no aparece en los medios —ofrezco al grupo.

Todos expresan su acuerdo. El grupo se abraza, sus miembros intercambian papelitos con teléfonos anotados a mano y *stickers* de sus organizaciones.

—Mañana tenemos una oportunidad. Nos vemos en el salón del Hyatt con nuestras máscaras.

Appelbaum sonríe con calidez. Algunos nos organizamos para compartir taxis y llegar a tiempo para el *cocktail* de apertura de Net Mundial en el Hyatt, en el otro extremo del mapa paulista. Mañana hay una oportunidad para alzar la voz, le dice al grupo con esperanza, y nos ofrece un mensaje de despedida:

—Es un placer conspirar con todos ustedes.

En el atardecer nublado de San Pablo, la brisa de abril ayuda a que el lugar esté repleto de jóvenes, niños y adultos que ocupan las mesas comunitarias que sirven para estudiar y jugar en los corredores del Centro Cultural San Pablo. Esquivamos

bailarines de *break dance* que ensayan una coreografía en la salida a la Rua Vergueiro. Los policías se mezclan entre ellos y nos saludan cuando pasamos la última puerta, de líneas rectas de hierro pintadas de azul.

En una hora, a las 8 de la noche, la organización de Net Mundial abrirá las puertas del Hyatt con un *cocktail* de bienvenida. Si queremos llegar a tiempo, estamos obligados a cruzar la ciudad más poblada de América del Sur en taxi. Decidimos compartir los viajes y me toca con Jérémmie, que aprovecha el camino para relajar el cuerpo antes de su próxima batalla. En su descanso, lo interrumpo: quiero saber cuánto ayudaron las revelaciones de Snowden a hacer más pública la lucha de los hacktivistas como él.

—Muchísimo. Sin Snowden no existiría Net Mundial. No estaríamos en Brasil con todos los funcionarios, las empresas y los activistas en el mismo lugar. La gente seguiría viendo el problema como «un problema de internet» y no como se comienza a ver ahora: como uno de libertad universal. Yo hace años que milito diciendo que la privacidad en internet es un derecho de autodeterminación sobre nuestras vidas. Mi aspiración era que en algún momento se viera como un tema que nos afecta a todos. Snowden nos dio un impulso gigante a las organizaciones, porque lo puso en el foco público, lo sacó de lo privado. El gobierno tuvo que salir a admitir que usa internet para espiar, cosa que ya sabíamos, ¡pero lo tuvo que decir!

Jérémmie respira, endereza la espalda, me pregunta sobre Buenos Aires, conversa con el chofer del taxi sobre radios de música brasilera. En sus viajes por América Latina, su pasatiempo favorito es comprar discos grabados a vendedores en la calle o en los subtes. Adora los CD «quemados», con tapas fotocopiadas en colores, de cumbia, salsa o reguetón. Luego los baja a su computadora y los sube en su blog, datalove.net, un repositorio de los gustos que suenan en el continente, y otra forma de militar por lo que cree: la cultura libre, aquella que se comparte entre muchas manos para circular y trascender los monopolios, las patentes, los *copyrights*. Pero no solo le importa la cultura latinoamericana, sino también el rol político del continente en las guerras de internet.

—Ustedes, América Latina, están tomando la iniciativa en temas de soberanía tecnológica. Es importante acompañarlos. Yo acá soy un francés más. Ustedes tienen que liderar la lucha por sus derechos de internet.

Aprovechamos los minutos que quedan del viaje para acicalarnos antes de entrar en el Hyatt: él rescata un saco de su mochila y se arregla el pelo. Jérémmie, como otros activistas reconocidos de internet, tiene un aura de *rockstar*. Entrar o salir de algún lugar con él es como hacerlo con una celebridad. La gente lo retiene, lo entrevista, le pide su clave de encriptación para mandarle alguna información, lo invita a una conferencia. Antes de bajar, uso los últimos minutos para cambiarme unas sandalias Birkenstock de periodista todo terreno por los zapatos que guardo en la mochila que ahora también alberga las máscaras de Snowden. Me maquillo con el espejo retrovisor del conductor, en los semáforos de la Rua Hungría.

Pasadas las 8 de la noche llegamos al hotel donde los organizadores de Net Mundial ofrecen la lujosa recepción de bienvenida. La seguridad es excesiva para la rutina habitual de un hotel en las afueras de San Pablo. Los turistas miran a los hombres de traje y *handy*, a las mujeres en *tailleur* o en ropas típicas de sus países, a los periodistas que ya entramos atentos. Somos los interesados en el rumbo que puede tomar internet en el mundo. Pero podemos pasar también por cualquier grupo de burócratas, activistas y cronistas que ingresan a un congreso internacional, toman tragos servidos en bandeja de plata y preguntan qué fue de su vida este año, embajador, ministro, profesor.

Nuestros nombres están en una lista. El de Jérémmie, en la sección de la «sociedad civil». El mío, en «prensa». Ya en la recepción, sobre las alfombras del Hyatt, las caipiriñas de maracuyá son el trago de la noche. Los anfitriones de la fiesta son los funcionarios del comité organizador de Net Mundial: la ICANN y el Comité Gestor de Internet (CGI) de Brasil, que reciben al resto de los asistentes. Hay CEO y representantes legales de empresas de telecomunicaciones y tecnología. Hay ministros de comunicaciones, funcionarios diplomáticos y delegaciones de los 97 países presentes. Hay académicos y periodistas. Y están los referentes de ese amplio espectro llamado «sociedad civil de internet», donde conviven organizaciones diversas, activistas y usuarios. En total, desde mañana y durante dos días de debates, serán mil doscientos participantes[97], entre los presentes en Brasil y los que contribuirán remotamente desde sus países.

El espectro de participantes es absolutamente diverso. Cada uno tiene sus intereses por discutir y defender. Pero el debate quedará para después. En este momento, es tiempo de caipiriña, de hacer chistes sobre los combates de mañana, como en cualquier reunión social o charla previa a un partido de fútbol importante. Jérémmie, Jake Appelbaum y otros activistas se acercan a Tim Berners-Lee y a Vint Cerf, dos eminencias de la Red siempre presentes en las reuniones. Aunque estén en distintos grupos, todos saben quién es quién. Se abrazan, se hacen chistes, se conocen de cada reunión de internet del mundo, pero también de cada discusión.

Entre los latinoamericanos, el guatemalteco Frank La Rue, todavía en su cargo de Representante Especial para la Libertad de Expresión de Naciones Unidas[98], concentra otro grupo muy concurrido, donde se comenta apasionadamente y se lo felicita por su reporte sobre la vigilancia de los Estados y su impacto en la libertad de expresión, publicado dos días después de las revelaciones de Edward Snowden. En el grupo de los organizadores, Fadi Chehadé, el CEO de ICANN, hace bromas con el grupo de funcionarios del gobierno de Brasil, encabezado por el ministro de Comunicaciones, Paulo Bernardo, y Virgilio Almeida, el secretario de Políticas de Tecnología del Ministerio de Ciencia. Entre ellos se gestó Net Mundial. Ellos pensaron y concretaron este encuentro que, desde mañana, estará en todos los medios

del mundo. Ellos, con la presidenta Dilma Rousseff a la cabeza, sostuvieron que Brasil era el país indicado para recibir a todos los involucrados en las decisiones de la Red.

Brasil, hoy, es la capital de internet.

A las 8 y media, en pleno *cocktail*, se escucha un aplauso sostenido, que incluye risas y felicitaciones destinadas a sus protagonistas: los funcionarios brasileros. La noticia se comienza a expandir entre los participantes: el Congreso acaba de aprobar en Brasilia el Marco Civil de Internet, después de cuatro años de discusiones, avances y retrocesos. La ley, que existía como proyecto desde 2009 con la idea de convertirse en una «Constitución de internet para Brasil», es una multirregulación de distintos principios que deben regir las actividades en la Red, como el respeto a la neutralidad, la libertad de expresión, la privacidad y la limitación de la responsabilidad de los intermediarios de contenidos como Google, Facebook o Microsoft para filtrar contenidos sin una intervención judicial previa. El proyecto implicó una gran movilización de los activistas por los derechos de internet en Brasil, que lograron superar el *lobby* de las empresas de telecomunicaciones en su contra, que objetaban la ley en el Congreso.

Con la aprobación del Marco Civil, Brasil se convirtió en el primer país del mundo con una ley integral sobre derechos de internet. La norma, coincidían incluso sus impulsores, era mejorable en muchos aspectos, pero era también el precedente y ejemplo de algo que se venía proponiendo en el mundo: crear marcos legales para proteger los derechos de los usuarios a medida que la Red se convierte en un nuevo espacio de conflictos. En contra de la opinión a veces general de que «no necesita ningún tipo de regulación», el Marco Civil fue especialmente bien recibido como un antecedente vital de que las reglas en internet sí podían ser discutidas, consensuadas, y en favor de los usuarios. «Se dice que las libertades de internet no precisan regulaciones. Pero sí las necesitan y el marco legal para ellas ya existe: son los Derechos Humanos que rigen para todo el planeta», dijo Frank La Rue. A él se sumó Tim Berners-Lee: «Estamos celebrando que el Senado brasileño haya aprobado la ley denominada Marco Civil de Internet, un gran ejemplo del papel positivo que pueden desempeñar los gobiernos para promover los derechos en la Red y mantenerla como un instrumento abierto. En Europa también están celebrando que el Parlamento Europeo haya aprobado una ley que protege los derechos de los internautas, incluida una forma de neutralidad de la Red[99]».

La aprobación del Marco Civil, además, llegó en el momento ideal. Fue la noche misma de la apertura de Net Mundial, cuando todos los participantes nos encontrábamos en el Hyatt. El brindis entonces no fue solo formal. Había una acción para festejar: Brasil estaba avanzando en sus planes de derechos digitales y con su nueva ley impulsaba a otros países a tomar cartas en el asunto. Sus funcionarios —

especialmente los del Partido de los Trabajadores o PT, que habían peleado en el Congreso por la aprobación de la norma— estaban eufóricos con la victoria. Pero no eran los únicos: para el resto de los activistas era un ejemplo de que los derechos de la Red sí podían ser regulados, a favor de los usuarios.

La ley de Marco Civil fue una de las victorias de Dilma Rousseff y de su país, Brasil, que entonces se ponía a la vanguardia de los países con una regulación moderna para los derechos en internet. Sin embargo, el camino que hizo que la potencia sudamericana se pusiera al frente de las discusiones de la Red no fue casual. Desde los hechos revelados por Edward Snowden en 2013, su gobierno, con ella como líder, había llevado el debate sobre el poder de internet a las portadas de los medios internacionales.

Desde junio de 2013, las revelaciones de Edward Snowden sobre el espionaje masivo de Estados Unidos a sus ciudadanos y los de otros países desencadenaron un efecto dominó en la política mundial. Nadie quedó fuera de la discusión y algunos gritaron tan fuerte que llegaron a mover las placas tectónicas de los continentes de internet.

Dentro de Estados Unidos, en enero de 2014, el presidente Barack Obama anunció una serie de reformas para otorgar mayor transparencia a las actividades de espionaje de la NSA. «No es suficiente con que esos programas tengan mi confianza, también el pueblo estadounidense debe confiar en ellos», dijo el líder norteamericano. Esa misma semana, Obama se había reunido para hablar de privacidad con Tim Cook de Apple, Randall Stephenson de AT&T y Vint Cerf de Google, tres de los altos mandos de las empresas de tecnología que —según los documentos de Snowden— habían facilitado los datos de sus usuarios a la Agencia de Seguridad Nacional. Sin embargo, fuera de Estados Unidos, el escenario era más difícil de controlar.

Cuando Snowden mostró que su país no solo recopilaba *mails* y llamados dentro de su territorio, sino que también espiaba a funcionarios, diplomáticos y hasta presidentes de otros países, las reacciones internacionales llegaron rápido y con un mensaje claro: el espionaje no es aceptable. En el Norte, Angela Merkel, la Canciller alemana, expresó la queja más furiosa de Europa: «Ya no estamos en la Guerra Fría», dijo, y pidió a Estados Unidos que aclarara los términos en que había vigilado a los alemanes y en particular a ella, a través de su teléfono celular personal. Ante la negativa de Estados Unidos de dar detalles sobre el espionaje, Merkel le dio un nuevo impulso a los proyectos de construcción de cables propios de fibra óptica y, en junio de 2014, anuló un contrato de su gobierno con la compañía estadounidense Verizon y eligió los servicios de telecomunicaciones de la local Deutsche Telekom.

En el sur, el enojo fue aún más fuerte y lo encabezó otra mujer, Dilma Rousseff. Tres meses después de las revelaciones de Snowden, la líder de una de las cinco potencias que conforman los Brics —el bloque con el 43 % de la población del mundo y el mismo PBI de Estados Unidos: Brasil, Rusia, India, China y Sudáfrica—

utilizó gran parte de su discurso en la Asamblea General de Naciones Unidas del 24 de septiembre de 2013 para demostrar su enojo. «Estamos ante un caso de invasión y sobre todo ante un caso de falta de respeto sobre la soberanía de nuestro país», dijo, mirando al frente, usando las cámaras que llevaban su mensaje a todo el mundo. Y agregó: «Brasil sabe cómo protegerse y redoblará sus esfuerzos para contar con leyes, tecnologías y mecanismos que nos protejan adecuadamente contra la intercepción ilegal de comunicaciones y de datos. Mi gobierno hará cuanto esté a su alcance para defender los derechos humanos de todos los brasileros».

Rousseff sabía que su pedido, al menos, sería escuchado. Su gobierno, junto con el de Lula Da Silva, había llevado a Brasil al lugar de potencia regional y mundial. En diez años, de 2003 a 2013, habían sacado de la pobreza a 35 millones de personas, y, en 2011, el PBI de su país había superado al del Reino Unido, convirtiendo a Brasil en la sexta potencia económica del mundo. Desde ese liderazgo económico y estratégico increpó Dilma a Obama. «Ya no son los únicos que pueden decidir sobre el mundo», fue su mensaje entre líneas.

De vuelta al Palacio del Planalto, Rousseff lanzó, entre septiembre y noviembre de 2013, una serie de iniciativas para fortalecer la soberanía tecnológica de su país. Y dijo con claridad algo que venía siendo escondido bajo la alfombra por años: ninguna decisión técnica de los gobiernos es neutral políticamente. Tampoco, y a la inversa, las decisiones políticas pueden tomarse sin mirar sus consecuencias tecnológicas. Eso no era posible antes y era mucho más improbable tras las noticias de Snowden, que comprobaban que las tecnologías son también un arma política de los Estados.

Dilma contraatacó: dijo que si el espionaje de gobiernos y empresas es inevitable, su país no se cruzaría de brazos y tomaría las medidas necesarias para evitar abusos a los derechos de la gente, no solo los digitales, sino también derechos humanos básicos, como informarse o crear conocimientos. En su plan de soberanía tecnológica, Rousseff volvió a impulsar la creación de redes de fibra óptica independientes de Estados Unidos, reflotó un proyecto liderado por su cancillería para combatir el espionaje y proteger recursos naturales estratégicos en colaboración con el Ministerio de Defensa de su vecina Argentina, promovió la instalación de servidores en su territorio, la creación de un servicio de *mails* propio con su correspondiente sistema de encriptación (abandonando el Outlook, el servicio de correo electrónico de Microsoft), y anunció que iba a exigir a empresas como Google o Facebook almacenar información de usuarios de ese país en servidores locales[100]. Y, tras cancelar una visita de Estado a la Casa Blanca, Rousseff buscó aliados internacionales para conformar un mapa del poder de internet que dependiera menos del poder de los Estados Unidos. El clima internacional, en especial el de las organizaciones de internet, no podía ser mejor.

El 7 de octubre de 2013, unos días después del discurso de Dilma en la ONU, en la Casa de Internet de América Latina, se reunieron las principales organizaciones del gobierno de internet (ICANN, ISOC y W3C, entre otras) y firmaron la «Declaración

de Montevideo sobre el futuro de la cooperación en internet[101]». En un edificio frente al mar, camino al aeropuerto de Montevideo, Uruguay, los organismos realizaron la primera declaración crítica a la forma de gobierno de la Red hasta ese momento y marcaron distancia de Estados Unidos tras las revelaciones de Snowden. El documento, recibido como histórico por la comunidad de la Red, expresaba, en uno de sus puntos: «La profunda preocupación por el debilitamiento de la confianza de los usuarios de internet a nivel global debido a las recientes revelaciones acerca del monitoreo y la vigilancia generalizados». Pero lo más importante era un llamado para que la ICANN, la organización más fuerte en el gobierno de internet, globalizara sus funciones, para que todos los actores, «incluyendo todos los gobiernos, participen en pie de igualdad». El mensaje era claro: el dominio de Estados Unidos sobre las decisiones de internet tenía que terminar o al menos abrir su juego.

Tres días después ocurrió una reunión cumbre. El 8 de octubre de 2013, Fadi Chehadé, el CEO de la ICANN, llegó a Brasilia. La excusa fue una visita al ministro de Comunicaciones, Paulo Bernardo. Pero finalmente la reunión también fue con Dilma Rousseff, semanas después de su discurso en la ONU. «Ella fue líder del mundo aquel día. Vine para agradecerle su liderazgo y discutir cómo partiremos de su visión para conseguir soluciones prácticas», dijo Chehadé, un libanés de 53 años, criado en Egipto y educado en informática y negocios en Nueva York. De personalidad decidida y carisma de líder en la comunidad de internet, al CEO de la ICANN no le fue difícil encontrar en Dilma Rousseff, otra estratega, una aliada para compartir su camino. Tras la reunión, ambos hicieron un gran anuncio: «El año que viene realizaremos un encuentro con líderes del mundo en Brasil para debatir la gobernanza de internet». Según los testigos de la reunión, Chehadé fue estratégicamente a buscar a la presidenta de Brasil, convencido de que América Latina liderará las discusiones sobre la soberanía de internet en las próximas décadas. Después del encuentro, nació Net Mundial.

La génesis del cambio estaba en marcha. Para Brasil y para América Latina era un triunfo. Para los organismos de internet, la posibilidad de abrir un espacio de diálogo luego de 25 años de dominio de Estados Unidos. Pero para el *establishment* norteamericano la noticia no era tan feliz. Tras el discurso de Dilma y el anuncio de la gran cumbre de internet en territorio latinoamericano, *The Economist* publicó un número especial dedicado a Brasil. En su tapa, el Cristo Redentor de Río de Janeiro aparecía prendido fuego, cayendo de un morro para estrellarse contra el suelo carioca. La excusa era la inflación y las protestas callejeras que había enfrentado el Partido de los Trabajadores unos meses antes. La culpa, por supuesto, era de Dilma. Un mes más tarde, *The Financial Times* fue aún más allá: «Brasil está yendo demasiado lejos con la seguridad de internet», titulaba el periódico del conservadurismo económico en sus páginas color salmón. Luego de advertir a la potencia del sur que no debía ponerse en contra porque «es segundo en cantidad de cuentas de Facebook en el mundo», la nota, sin firma pero abrazando las ideas del medio, seguía: «El proteccionismo de

Rousseff con la web es malo para su país. Le resta competitividad y daña a su sector tecnológico. Va a sufrir. Rousseff debería pensarlo de nuevo».

Pero Dilma siguió adelante. En abril de 2014, abrió las puertas de su casa para recibir a la comunidad de internet.

Durante el *cocktail* de inauguración de Net Mundial, se confirmó otra noticia: la presidenta de Brasil estaría presente la mañana siguiente en el Hyatt, para dar el discurso de bienvenida que todos esperaban como la continuación de su pedido de soberanía político-tecnológica en la Asamblea de la ONU. La recepción terminaba con el anuncio de un día agitado. Pero antes restaba una noche de descanso en el hotel y custodiar las máscaras de Snowden para que llegaran a los hacktivistas al día siguiente.

Ya en la habitación enorme, con vistas al Shopping Morumbi, me acosté después de un día de 16 horas, pero sin despegar los ojos de mi mochila, tirada sobre la mesa, con las máscaras. Aunque mi cuerpo quería dormir, me levanté para llevar más cerca de la cama la bolsa que guardaba las máscaras que al día siguiente serán fundamentales para la protesta. Casi sonámbula, caminé por la alfombra iluminada por las luces del *shopping* que atravesaban el ventanal. Rescaté la mochila y la dejé a mi lado, adentro de la mesa de luz. Tenía en mis manos una responsabilidad: la cara de un hombre de mi generación que hacía unos meses, en Hong Kong, había dicho que no quería vivir en un mundo controlado, donde la tecnología fuera un arma aplicada sin consenso de la gente. Estaba con él. Pensaba como él. Soy de su generación, de la que todavía cree que la privacidad es un derecho básico, que es importante para muchas otras cosas, entre ellas para decir lo que pensamos, para hacer política. Por esa razón, esa noche debía cuidar las máscaras de Snowden que me habían confiado para que la mañana siguiente aparecieran en todos los medios del mundo.

El 23 de abril, la cita es a las 9 para la acreditación formal de Net Mundial. El aviso es llegar temprano al Hyatt. Dilma estará allí a las 10. La seguridad presidencial es extrema e ingresar se convierte en un trámite engorroso. A las 9.45, los alrededores del hotel, que incluyen la sede paulista de la red de medios O Globo, se inundan de custodios. El operativo de seguridad anula toda señal en los celulares: está llegando la presidenta de Brasil para abrir formalmente el encuentro.

La fila de invitados y periodistas frente al mostrador de acreditaciones todavía es larguísima. Quiero entrar ya, pero me pido paciencia. La organización brasilera es seria. Lejos de la imagen turística siempre sonriente del país, la producción del encuentro trabaja con postura y modales circunspectos, casi austeros. Desde el comité de prensa hasta la seguridad, todos se desenvuelven con una eficiencia que parece

decirle a los funcionarios e invitados del mundo que Brasil puede encargarse de una reunión de alto nivel con total destreza. Incluso, con retos y modales serios cuando se acerca la llegada de Dilma y la fila aún avanza con lentitud.

Termino la acreditación y llega el momento de pasar la mochila por el escáner de seguridad. Antes de apoyarla en la cinta, le sonrío al guardia. Adentro tengo las máscaras de Snowden, así que la apoyo y la tapo con el saco que llevo encima con la excusa del aire acondicionado del hotel. Afuera suenan las bocinas de la comitiva. Dilma ya está aquí. La seguridad se acrecienta. Me revisan el grabador, el cargador de baterías, los bolsillos del saco. Pero la pila de máscaras, todavía dentro de la bolsa de supermercado pasa sin ser detectada. Al guardia le parecen papeles o simples fotocopias. Me pongo el saco, cargo la mochila y entro en la recepción. La primera parte de mi misión está cumplida.

En el área de periodistas quedan unos pocos lugares; el salón está completo. Todavía tengo que entregar las máscaras. Levanto la vista y veo a Mishi, la activista de la India de quien me hice amiga ayer, caminando hacia mí en medio del salón. Me saluda con un abrazo y se queda de pie al lado de una mesa repleta de termos de café y vasos de agua descartables. Me da charla para no despertar sospecha, me habla de nuestros peinados, mientras los asistentes terminan de desayunar rápido antes de la entrada de Dilma. En medio del gentío, saco la bolsa con las máscaras y se la entrego. Ella, alojada en el Hyatt, pudo ingresar al salón con una tijera. Se acerca a la ventana, lejos de la multitud y la saca de su cartera de brillos y colores orientales: recorta el perímetro de las caras de Snowden y, en unos minutos, ya tenemos las máscaras listas para la acción. Net Mundial puede comenzar.

En el Hyatt de San Pablo, de alfombras cálidas y vasos con agua de manantial embotellada dispuestos en mesas con manteles blancos de puntilla, la *crème* de la diplomacia mundial de internet, incluidos los inventores de la Red, toma asiento en las sillas de pana de la sala de conferencias más grande y lujosa del hotel. Los funcionarios de los gobiernos, también invitados, dominan las primeras filas. En la columna de la izquierda, los activistas y defensores de los derechos de los usuarios cubren en bloque otra parte del espacio. Todos compartieron tragos, risas y anécdotas la noche anterior. Todos se conocen, pero hoy cada uno toma su rol. Son casi las diez de la mañana del 23 de abril de 2014 y el cronograma está atrasado.

Cerca de las 11, un tumulto. Dilma ingresa al salón. Saluda a las autoridades y da la señal de comenzar. Entonces se apagan las luces. Y aparece *ella*, en una pantalla de 20 metros. Brillante, precedida por los ruidos de las conexiones, unos «bips» como sinapsis de fibra óptica (que en la realidad no existen, pero que en la imaginación de todos acompañan a la luz en su viaje supersónico por los cables hasta llegar a las computadoras). Entre azules y verdes, rebota en la pantalla y tiñe la mirada de todos.

Con ustedes, internet.

El video de apertura es como uno de esos compilados que les hacen a las chicas para su cumpleaños de 15. Sus mejores momentos: el paso a paso de sus felicidades hasta llegar a hoy. Y es tan linda, e hizo tanto por nosotros, que nos encanta. Tiene un poder. Nos tiene en la palma de la mano. Como una diosa, internet nos encanta a todos.

Internet encanta a cada uno por una razón distinta. A sus casi tres mil millones de usuarios porque nos ofrece una ventana permanente para mirar (o espiar) el mundo, hablarle a cualquier ser humano del planeta, hacer cosas que antes nos llevaban horas en apenas minutos, encontrar información, descubrir lugares, donar a una buena causa o ejercitar un vicio oculto con la misma facilidad. A las empresas, porque están más cerca de la gente, es decir, de sus clientes, en cuyas vidas se pueden inmiscuir para venderles sus productos. A otras empresas, más grandes, porque ganan mucho dinero construyendo y manteniendo la infraestructura del monstruo de internet en funcionamiento. A los países, democráticos o autoritarios, la Red a veces les encanta y a veces les disgusta: les permite estar más cerca de sus ciudadanos, pero al mismo tiempo les abre a ellos un mayor poder de expresión y reclamo. Otras veces, a los Estados, a las empresas y a cualquiera que domine el arma internet, los hace caer en la tentación del espionaje o la censura para controlar vidas, perseguir terroristas o simples disidentes. Y así es para todos: a cada ser humano, a cada profesión, a cada grupo antes ignoto y ahora escuchado, a cada artista que consigue la fama por YouTube, a cada político que captura seguidores en las redes sociales, a cada activista que logra que su mensaje se expanda, internet lo cautiva. Su poder complace a todos.

Luego del compilado con el que dio inicio la conferencia, Dilma Rousseff, en un sobrio saco y pantalón negros con una pequeña franja blanca, zapatos bajísimos a tono, promulga con su firma la ley de Marco Civil. Sonríe con orgullo de su país avanzando en nuevos derechos, antes de comenzar su discurso de apertura. Con las manos decididas apoyadas sobre el púlpito, ahora repite gran parte de su discurso en la ONU condenando la vigilancia masiva. El aplauso del público es intenso.

La apertura sigue su curso. Sin embargo, Carl Bildt, el ex Primer Ministro sueco y contra quien habíamos organizado la acción de las máscaras de Snowden, finalmente no aparece en Net Mundial. Pero las caras de Snowden ya están en la sala y dicen presente. Hacia el final del discurso de Dilma, Jérémmie Zimmerman y el resto de los activistas cubren sus rostros con las máscaras del exempleado de la NSA, formando una hilera de Snowdens que interpelan a todos los participantes de la gran reunión de internet.

Son pocos: seis hombres y mujeres en un auditorio de cientos. Pero es imposible no mirarlos. Están aquí para advertir que internet no es solo un invento para conectar y hacer el bien en el mundo. Con sus máscaras, recuerdan a todos los presentes que también la Red puede utilizarse para el mal. Señalan al estrado y luego dirigen su mirada hacia los fotógrafos de las agencias del mundo que los retratan para hacer llegar la imagen a todos los rincones del planeta. También apuntan a los periodistas.

Y entonces, me pongo de pie. Tengo que sacarles una foto que registre el momento de la protesta. Pero no es sencillo. Los custodios presidenciales mantienen a la prensa en su lugar, evitan el revuelo de las cámaras que disparan hacia los activistas con el rostro de Snowden. La misión se hace tan complicada que, tras sacar una foto con mi tableta en alto, sin mirar si había quedado bien, dos hombres de seguridad de repente me toman de los hombros y me devuelven a la fuerza a mi asiento. El intercambio entre mi español, el portugués de ellos y un inglés poco conciliador termina con una cortesía impostada. Pero ya tengo la foto. Y las redes sociales comienzan a bullir con la imagen de los activistas con sus máscaras de Snowden. Al rato, también las agencias de noticias norteamericanas dan cuenta de la protesta. El objetivo está cumplido.

Tras unos minutos de tensión y empujones, la presidenta de Brasil termina su discurso. Impone su voz y calma el murmullo. Con su mirada en las máscaras, les dirige unas palabras a los activistas que levantan la cara de Snowden: no es a ella a quien tienen que reclamar. Y va más allá cuando se ofrece a ser líder en el pedido por la soberanía de los países que no toleran el espionaje masivo como arma de la política internacional. Con su voz decidida, se adueña del lugar. Termina un discurso serio, tras el cual invita al resto de los participantes a tomar acciones para que esto suceda.

Durante dos días, el encuentro sigue su camino sin descanso, con reuniones, presentaciones sobre el futuro de internet. Los funcionarios, empresarios y activistas tienen el objetivo de llegar a un documento de acuerdo final, a «una hoja de ruta», en la jerga de los encuentros internacionales. Sin embargo, arribar a ese compromiso no es tan complejo como gobernar internet, un bien que pertenece a sus usuarios, pero también a empresas y gobiernos, cada uno con sus intereses. «Nosotros, los ciudadanos, somos todos copropietarios de internet, si la consideramos como la suma de su infraestructura, sus tecnologías y, mucho más importante, como la suma de actividades, datos y contenidos, todos contribuimos a que exista», escribió Jérémmie Zimmerman el día de la inauguración de Net Mundial. En su planteo anida una idea ahora más compartida, que será la base de la política de la Red en los próximos años: internet puede y debe ser considerada un bien común.

Como la paz mundial, como el medio ambiente, como la cultura, los bienes comunes de la Humanidad deben ser protegidos porque también son amenazados. Lo que es importante para todos también es disputado por todos. Por eso genera guerras. Entonces, ¿cómo ponerse de acuerdo y defender un arma tan distinta, con tantos usos posibles? En los encuentros como Net Mundial, como en la Conferencia de Yalta tras la Segunda Guerra Mundial, sus líderes se reúnen para sentar los acuerdos de la paz después de una guerra. Aunque, en la Red, las guerras todavía están sucediendo. En esta guerra fría tecnológica, además, las decisiones son más difíciles, porque ya no se trata de que se pongan de acuerdo los presidentes de cada país, sino también las

instituciones que gobiernan la red, las empresas y los usuarios. ¿Cómo gobernar para toda esa humanidad que usa internet en sus miles de formas posibles? ¿Cómo establecer leyes que luchen contra el crimen o la pedofilia *online* en un mundo con culturas y legislaciones locales donde la pedofilia y el crimen significan cosas distintas en cada país? ¿Cómo definir reglas para que internet no limite la libertad de expresión, cuando todavía hay países donde la libertad de expresión está cercenada o disputada entre diversos actores? ¿Cómo regular las ganancias de las empresas de tecnología en un mundo donde el lucro lo es todo? ¿Cómo pensar en proteger la privacidad o estar atentos a la vigilancia masiva de los ciudadanos cuando la gran maquinaria del entretenimiento nos dice que mirar y ser mirados las 24 horas es todo lo que necesitamos para ser felices?

El jueves 24 de abril, a las 18 BRT (hora de Brasil), salió a la luz el primer borrador del documento alcanzado luego de 48 horas de intensas reuniones entre todas las partes interesadas. Durante la siguiente hora y media, todo fue corridas, negociaciones de último minuto (tal vez las únicas que finalmente importan, porque son las que demuestran dónde están los verdaderos conflictos), rumores de pasillo y falta de café. A las 19.31, cuando se presentó el escrito final**[102]** de la reunión, llamado «Declaración Multisectorial de Net Mundial», todos bebían agua. Pero había problemas más graves. Durante las últimas horas, tres puntos de la declaración no terminaban de convencer a las partes: neutralidad de la Red, vigilancia masiva y derechos de autor. Allí estaban las guerras más difíciles.

Al término de Net Mundial, ninguna de las «múltiples partes» quedó conforme con el documento. Las empresas salieron con algo más de ventaja, y llevaron a la sociedad civil, el sector más ruidoso —tanto en el encuentro como en murmullo de las redes sociales— a decir algo muy repetido: «Estos encuentros solo sirven para perpetuar el *statu quo* del poder de internet». En el documento final no se hablaba de la neutralidad de la Red, un reclamo de los grupos de usuarios a las empresas y los Estados para protegerla con legislaciones nacionales. La otra parte, la sociedad civil logró incluir las palabras «vigilancia masiva», para que los países declararan «revisarla», tanto si la aplicaban los Estados o las compañías privadas.

Sin embargo, la reunión sentó un precedente en las discusiones de la Red. Un país líder de América Latina (antes llamado del Tercer Mundo; ahora parte de los Brics) era sede de una gran reunión para discutir que internet también es un ámbito de la política internacional. El mundo, al menos por un momento, se enteró de países que se comprometían a respetar la privacidad de la Red y que su poder, hasta ahora concentrado, estaba siendo cuestionado por algunos Estados antes dejados de lado en las decisiones mundiales, pero que hoy tienen un gran peso en el desarrollo futuro de las tecnologías.

Pero las guerras de internet recién comienzan. Y no se definen en documentos, sino en escenarios reales: reuniones internacionales, legislaturas y parlamentos de los países, estudios de abogados, redes sociales, protestas en la calle, ataques de

hacktivistas y contraataques de ciberejércitos. Como toda discusión política, suceden bajo presiones y *lobbies* de los actores interesados. Como me decía un funcionario de un organismo de internet en una pausa de las negociaciones: «Esto es como *House of Cards*». De las misma forma que en la serie protagonizada por Kevin Spacey y producida por Netflix, donde hay poder hay movimientos sucios, negociaciones a puertas cerradas y comunicados de prensa que ocultan operaciones. Es lógico: los intereses de la tecnología son tan pesados como los países y las corporaciones que quieren dominar la tecnología para controlar, proteger, dar libertad, quitarla, ganar dinero, tantos fines como intereses permita la Red. La paz no existe.

Terminadas las reuniones internacionales, cada actor de la guerra vuelve a su país, a la lucha local. Las leyes se definen en cada país como cualquier lucha política. Los activistas tienen allí su papel más importante. Las empresas contratan allí sus mejores abogados. Los legisladores tienen que entender problemas que antes no entendían, los jueces definir conflictos que no estudiaron en ninguna facultad, los periodistas tenemos que explicar temas que antes no eran parte de la agenda pública. Y los usuarios, idealmente, tenemos que entender las guerras de internet. Porque somos parte de ellas. Porque las guerras son de todos, son un nuevo problema para los ciudadanos. Porque si las entendemos como temas individuales nunca serán debates públicos.

VII

Toda la Red es política: usuarios, empresas y gobiernos luchan por la web

> «A medida que los Estados se fusionan con internet y el futuro de nuestra civilización deviene en el futuro de internet, estamos obligados a redefinir las relaciones de fuerza».
>
> JULIAN ASSANGE.
> *Criptopunks* (2012).

> «Internet no es solo el mejor servicio de video del mundo.
> No es simplemente una mejor forma de ver pornografía.
> No es solo una herramienta para planear ataques terroristas.
> Estos son solo casos del uso de la Red. Pero ella es el sistema nervioso del siglo XXI.
> Es hora de que empecemos a actuar así».
>
> CORY DOCTOROW[103].

En 2007, a los 27 años, Claudio Ruiz, chileno, ya recibido de abogado, se dio cuenta de que tenía que tomar una decisión. Había terminado la facultad y trabajaba en Derechos Digitales, una organización que había fundado con algunos de sus compañeros. Los primeros años escribían *policy papers*, documentos serios y académicos sobre cómo tratar los nuevos problemas legales que se presentaban con la Red. Pero, en mayo de ese año, la presidenta Michelle Bachelet envió al Congreso Nacional una propuesta para reformar la Ley de Propiedad Intelectual de 1970, en donde se incluían varios puntos relacionados con internet. La ministra de Cultura convocó a Claudio y su grupo, ya con experiencia en derechos de autor en la Red, como asesores. La presión era grande: la reforma se proponía en el marco de la negociación de un tratado de libre comercio con Estados Unidos en el cual la potencia buscaba flexibilizar los acuerdos de *copyright* para beneficiar a su industria.

—Tuvimos que tomar una decisión. Nos llamaron para trabajar asesorando a la ministra de Cultura en temas de derechos de autor. Pasamos de ser buenos técnicos a

involucrarnos en una negociación «real» y entender sus códigos. Nos costó, pero meternos en política fue lo mejor que pudimos hacer.

Claudio Ruiz, hoy con 35 años, recuerda aquel momento mientras desayuna un café con leche con medialunas en El Banderín, un bar de Almagro. De espalda ancha y una barba espesa que le cubre la mitad de la cara, Claudio se entusiasma hablando de *su* tema, internet.

—Yo me gano la vida luchando por las cosas que creo: defender los derechos humanos en el ámbito digital. Eso es grandioso. Pero aprendí que para lograrlo tengo que jugar el juego de la política.

En las guerras de internet, Claudio forma parte de un colectivo grande y diverso llamado «sociedad civil». Dentro de él conviven todo tipo de organizaciones que reclaman y luchan, con diferentes herramientas, por la aplicación de derechos y libertades en la Red. Entre ellas también existen diferencias a la hora de pelear las guerras y sobre qué rol tomar frente a los distintos actores que controlan la Red. El primer grupo, más cercano al anarquismo, propone evitar cualquier control: internet no debería estar en manos de nadie (ni empresas ni países); debería funcionar en estado de total libertad. Para el segundo grupo, que podríamos llamar «liberal», la intervención debería darse para proteger los derechos y las garantías que tenemos como ciudadanos en el ámbito *online* y de reclamar transparencia absoluta de la información como forma de llegar a la libertad de expresión. Para un tercer grupo, más cercano al marxismo o a una visión de lucha política pragmática, la Red es otro ámbito de una disputa del sistema capitalista mismo: para ellos, no existen conflictos *solamente* de internet, sino que son parte de una batalla más amplia (y antigua) sobre quién se queda con qué o cómo se distribuyen mejor los recursos. Sostienen que si la intervención es necesaria para regular desigualdades que produce el mercado, es bienvenida. Por supuesto, para todos ellos, hay luchas comunes, donde unen fuerzas.

Entre estas perspectivas, Claudio se ubica en una posición pragmática que no reniega de la política. Acepta el diálogo y que ninguna guerra puede pelearse fuera de un contexto de luchas de intereses. Sabe que hay que dialogar con todos los involucrados, e incluso educar a ciertos sectores o personas que no tienen por qué conocer sobre todos los temas, algo que sucede a menudo con los problemas de la tecnología.

—Desde las organizaciones de la «sociedad civil» de internet necesitamos entender los códigos de la política para lograr pequeños o grandes cambios.

Claudio lo explica con un ejemplo: cuando se empezó a negociar el Acuerdo Transpacífico de Cooperación Económica (TPP), un tratado de libre comercio multilateral que Estados Unidos promueve y negocia en secreto con once países del Pacífico, su organización sabía que, entre otros efectos, se iban a socavar los derechos de los chilenos en internet. Pero su campaña no se propuso enfrentarse a todo el acuerdo, porque implicaba una lucha política inmensa. En cambio, idearon un

eslogan («No al TTP cerrado») para decirle a la gente que Chile estaba negociando un acuerdo en secreto, donde también se escondían violaciones a sus derechos *online*.

—En vez de explicar todo el palabrerío de la ley, hicimos claro que con el TPP los proveedores de internet podían censurar contenidos sin intervención judicial, endurecer las sanciones a las infracciones del derecho de autor por compartir un video con un amigo o intervenir en el intercambio de información privada.

Lograr que los usuarios comprendan la importancia de las guerras de internet en sus vidas es una parte de su trabajo. Pero Claudio también sabe que además se necesita educar a los políticos mismos, que muchas veces tienen que decidir sobre problemas nuevos que avanzan a medida que lo hace la tecnología.

—Hay activistas que cometen un error grande cuando dicen «todos los diputados son unos ignorantes en temas digitales». Bueno, hay ignorancia en general sobre asuntos nuevos. De la misma forma en que no le pedimos a un legislador que sepa todo sobre la ley de aguas o el código penal sin informarse con sus asesores, tampoco podemos pretender que sepa todo sobre la neutralidad de la Red. Hay asesores, gente que te puede explicar. Lo importante es dar el debate y no cerrarlo. Por ejemplo, cuando hablamos de propiedad intelectual en internet, les planteamos a los diputados preguntas que tuvieran que ver con su vida real: «¿Tu hijo comparte fotos por Twitter o por *mail*? ¿Sabes que solo por compartir una imagen podría ser considerado un delincuente e ir preso?». Desde esa pregunta, es más fácil hablar: cómo te afecta a vos la guerra, cómo toca tus derechos.

Su experiencia también le hizo a Claudio ver de cerca que si el debate no se abría a la sociedad, quedaba en manos de las grandes corporaciones de la tecnología que destinan grandes recursos para favorecer sus intereses.

—Si nosotros no hablamos de esto sencillamente, las grandes empresas se encargan de hacer *lobby* para convencernos de que si compartimos una foto somos delincuentes. La presión de la industria es muy poderosa y el dinero que destina a publicidad, *marketing*, viajes, fiestas, enorme. Por eso también nos valemos de armas que sí dominamos, por ejemplo, las redes sociales y la movilización digital.

La primera movilización *online* masiva de las guerras de internet sucedió en enero de 2012. Frente a la discusión en el Congreso de Estados Unidos de las leyes SOPA (Stop Online Piracy Act) y PIPA (Protect IP Act), que buscaban limitar y sancionar el intercambio en internet por motivos de derechos de autor, la Red se organizó en una protesta conjunta de usuarios y empresas. A través de un apagón, llamado #SOPABlackout, se unieron grupos de usuarios de todo el mundo, organizaciones como Mozilla y Wikipedia, y hasta megacorporaciones como Google, eBay y Facebook. La protesta fue un éxito: 15 congresistas cambiaron su postura frente a SOPA y la ley postergó su tratamiento. Solo en la primera hora de la protesta, el 1 % de los tuits mundiales se referían al tema y la portada de Wikipedia, que explicaba cómo podía ser un mundo sin conocimiento libre, fue visitada por 162 millones de personas y comentada por 12 mil. En un comunicado, la Casa Blanca

sostuvo que el gobierno de Barack Obama no apoyaría «una legislación que reduzca la libertad de expresión». Los gigantes de internet también firmaron una carta de oposición rotunda al proyecto. Pero quizá el logro más grande del reclamo fue que, por primera vez, la libertad de internet se transformaba en un tema de discusión en los medios y en las redes sociales.

Las batallas por las guerras de internet se hacían cada vez más públicas, impulsadas por el efecto WikiLeaks y la organización de activistas. Luego las revelaciones de Snowden las hicieron estallar nuevamente, con la prueba de que los abusos a la privacidad de los usuarios eran perpetrados por las mismas instituciones que tenían que protegerlos. Hoy, las guerras no solo ocupan las portadas de los medios *online* o las redes sociales, sino que llegan a las tapas de los viejos medios de papel y a ocupar minutos en los noticieros de la noche.

Para algunos, como Claudio Ruiz, o como yo, las guerras son más claras o más fáciles de comprender. Nuestra edad (los dos tenemos 35 años) tiene mucho que ver. En su libro *El fin de la ausencia*, el periodista canadiense Michael Harris escribe que los que vinimos al mundo antes de 1985 somos los últimos de una especie. «Si naciste antes de 1985, entonces sabés cómo es la vida con y sin internet —dice—. Podés hacer la peregrinación entre Antes y Después». Harris, como nosotros, nació en un mundo diferente, con menos canales de comunicación, menos formas de entretenimiento, menos escrutinio público de todo lo que hacemos o sentimos. Y, según él, no es un mundo ni mejor ni peor, pero nos ofrece una posición privilegiada para comprender los conflictos actuales y los que se acercan: «Si somos las últimas personas en la historia en conocer la vida antes de internet entonces también somos los únicos que podremos hablar, para siempre, ambas lenguas. Somos los únicos traductores que podemos interpretar fluidamente el Antes y el Después[104]».

Hoy, las discusiones sobre la tecnología forman parte no solo de las noticias, sino de las conversaciones con nuestros amigos o en la mesa familiar. Las guerras de internet ya no son del futuro. No solo se debaten, sino que también empiezan a provocar consecuencias reales, enfrentamientos entre presidentes y protestas en la calle. Las guerras de la Red salieron de los aparatos.

¿Cuáles son esas luchas de las que escucharemos hablar en los próximos años? ¿Cómo hacer un mapa de ese campo de batalla para saber dónde estamos parados —o dónde quisiéramos estarlo— en esas luchas? ¿Cómo traducirlas para no quedar atrapados en medio de uno y otro poder? Primero, explicándolas desde lo técnico y lo político, pero también desde sus orígenes históricos, para entender quiénes conforman cada ejército. Aquí, algunas de esas guerras[105].

La guerra por las rutas.
Geopolítica: países, corporaciones y el control de la información.

La primera es una guerra geopolítica que condiciona el campo en donde ocurren el resto de las batallas. Se trata del enfrentamiento por el control de las rutas de la información, los caños, los tubos y los servidores que todos utilizamos para transportar y albergar nuestros datos. Por allí pasa todo en forma de bits: lo público y lo privado; desde los videos más ingenuos de gatitos en YouTube hasta los secretos de Estado más delicados.

La publicidad nos hace pensar que la información en internet puede tomar infinitos caminos pero la realidad es que, como dice el sociólogo Mariano Zukerfeld, «los tendidos submarinos de fibra óptica, los *backbones* continentales y los satélites pertenecen a unas pocas empresas que oligopolizan la circulación de los flujos de información digital[106]».

Esa base física de internet, sobre la que se erige el resto de su estructura, tiene pocos dueños que ejercen un gran poder, similar al que detentan quienes dominan las rutas de otros bienes preciados. «Con el control de los cables de fibra óptica, por donde pasan los gigantes flujos de datos que conectan a la civilización mundial, ocurre lo mismo que con los oleoductos. Este es el nuevo juego: controlar la comunicación de miles de millones de personas y organizaciones», dice Julian Assange en el prólogo de su libro *Criptopunks*. En América Latina, esos caminos de la información pasan, en un 98 % por cables, servidores y empresas de Estados Unidos[107], con lo cual hay un claro problema: las comunicaciones están en cada país, pero también están en el territorio de una superpotencia[108].

El resultado de este mapa concentrado es una serie de batallas de soberanía, un campeonato de TEG del poder digital. Si nuestros datos pasan por otras manos y fronteras nacionales, ¿quién decide por ellos, qué ley les corresponde, quién puede controlarlos, espiarlos o utilizarlos? La infraestructura de internet hoy es un territorio que también puede ser atacado para dañar al adversario. O utilizar los datos que pasan por esas vías para lograr un objetivo político: espiar las acciones de otro Estado, a sus propios ciudadanos, desviar informaciones, apropiarse de documentos que permitan tomar decisiones sobre ataques, guerras o disputas diplomáticas. Durante la Guerra Fría era necesario recurrir al espionaje, pero ahora todo está en una serie de caños y servidores que, por el crecimiento de internet en un país (Estados Unidos) y en una serie de corporaciones (generalmente, también de ese país), resultan en una nueva concentración del poder en pocas manos (y la tentación de controlarlo para dominar a otros). Así lo dice Assange: «El Gobierno de Estados Unidos no ha mostrado muchos escrúpulos en transgredir su propia ley al interceptar estas líneas para espiar a sus propios ciudadanos. Y no existen las leyes que impidan espiar a ciudadanos extranjeros. Cada día, cientos de millones de mensajes de toda América Latina son devorados por las agencias de espionaje de Estados Unidos y almacenados para siempre en depósitos del tamaño de ciudades. Los aspectos geográficos relativos a la infraestructura de internet, por lo tanto, tienen consecuencias para la independencia y soberanía de América Latina».

Por supuesto, los usos —y abusos— de la infraestructura de la tecnología se realizan de acuerdo con un mapa de disputas de poder que pelean por otros motivos, especialmente los económicos y los estratégicos. Son luchas de poder de un mundo hasta hace unos años dominado por Estados Unidos, pero que ahora tiende hacia una diversidad de actores, que aunque todavía están lejos del poderío militar (el poder duro) de los Estados Unidos[109], pueden comenzar a disputar un poder blando, con el conocimiento y manejo de otras herramientas basadas en la tecnología. No por casualidad, China y Rusia —dos líderes del bloque Brics— participan activamente en las reuniones de gobernanza de internet, casi siempre con expresiones de disidencia y destinan grandes presupuestos a la inversión en infraestructura tecnológica propia. En San Pablo, tras la lectura del documento final de Net Mundial, un representante de la comitiva de Rusia subió al estrado y expresó no solo su completo desacuerdo con la declaración final, sino también con la forma en que se habían tomado las decisiones. Pero allí estuvo su delegación para participar del debate.

En los últimos años, los países que alientan un mapa del mundo multipolar, como Brasil y el grupo de los Brics, o algunas naciones latinoamericanas, iniciaron dos ofensivas. La primera es diplomática y consiste en denunciar a los grandes poderes, especialmente a Estados Unidos, por utilizar la gran infraestructura de comunicaciones para entrometerse con sus datos: ya sea espiando a ciudadanos, posibles disidentes o terroristas, como a los funcionarios, diplomáticos y hasta presidentes de todo el mundo, sean amigos de la potencia o sus enemigos. Eso fue lo que denunció Dilma Rousseff (y aunque su país también hubiera espiado a diplomáticos norteamericanos[110]).

La segunda ofensiva la están dando en el desarrollo de redes propias de infraestructura, independientes del control de los Estados Unidos y las grandes potencias del mundo. Con esto y con el control de sus propios servidores de datos y *software* para el manejo de la información, reclaman una parte de la soberanía que, en las primeras décadas del avance de internet, quedó en manos de un puñado de empresas e instituciones fuertemente vinculados con el gobierno y la estructura militar norteamericana. El más ambicioso de estos proyectos es el Brics Cable, que unirá a Brasil, Rusia, India, China y Sudáfrica, enlazando Vladivostock en Rusia, Shantou en China, Chennai en India, Singapur hacia Ciudad del Cabo en Sudáfrica y cruzando el océano hasta Fortaleza, Brasil. Sin embargo, esto no promete una solución totalmente soberana, ya que, de todas formas, si cualquier ciudadano ruso, brasilero o sudafricano utiliza servicios como Facebook o Google, sus datos igual viajarán por servidores de estas empresas, mayormente ubicados en Estados Unidos.

En esta batalla, el avance o el retroceso será también en el plano de la geopolítica, de las negociaciones y alineaciones internacionales, en un mundo que está dejando de tener un solo centro (Estados Unidos) para tener una serie de potencias que lideran en el mundo. Para ellas, dominar las vías de comunicación de la tecnología será estratégico.

Sin embargo, también en los próximos años veremos crecer un nuevo fenómeno: las guerras de la política internacional se dirimirán no solo con ejércitos reales, en campos de batalla de tierra o mar, sino que también se pelearán en espacios virtuales, de la mano de los ciberejércitos que cada país viene formando en los distintos (ciber)territorios de la Red. Desde las grandes potencias hasta países más pequeños con voluntad de imponerse en la agenda internacional o de producir daños y defenderse de ataques, distintos Estados reclutan y entrenan, desde hace unos años, *hackers* y expertos en ciberguerra. Más o menos reconocidos oficialmente por los gobiernos, todos ellos dependen de las estructuras militares o departamentos de defensa de cada país y son financiados tanto en su trabajo como en sus sofisticadas infraestructuras por el presupuesto nacional. Las cibermilicias también compran armas, pero en forma de infraestructura de telecomunicaciones: computadoras, servidores y *software*.

En 2010, Estados Unidos fue uno de los primeros países en hacer público su ciberejército, también conocido como United States Cyber Command, que depende directamente de las Fuerzas Armadas y declara la misión de «velar por los intereses del país y sus aliados, con la protección directa a sus sistemas informáticos o actuando en respuesta a ataques». El Cibercomando trabaja en conjunto con la NSA y ambos tienen su sede en Fort Meade, Maryland, aquel lugar por donde Edward Snowden pasaba por en frente durante la adolescencia y que luego fue su lugar de trabajo hasta revelar la información sobre la Agencia de Seguridad. En su página oficial, arcyber.army.mil, además de detallar sus tareas y noticias, los candidatos a integrar el cuerpo pueden postularse, bajo un llamado: «Se necesitan cibersoldados. Queremos reclutar y desarrollar a los ciberguerreros del siglo XXI. Apasionados, creativos y determinados a encontrar soluciones a los desafíos que enfrentamos en el siglo». El Comando ya cuenta con cinco mil soldados, que, al ser Estados Unidos el país más atacado —por lejos— por ciberofensivas de otros países, tiene la misión de defender sus territorios virtuales.

El segundo ciberejército más poderoso está en China. Llamado Ejército Azul o «Unidad 61398», depende del Ejército Popular de Liberación (las Fuerzas Armadas del país) y cuenta con unos dos mil integrantes y una infraestructura de fibra óptica provista por la estatal China Telecom. El 80 por ciento de sus ataques están destinados a compañías de Estados Unidos, en especial las de la categoría «blue chip» (grandes corporaciones que cotizan en bolsa), y para defenderse de los ataques a sus instalaciones. En cuestiones defensivas, Israel, Finlandia y Suecia encabezan el *ranking* de los países más preparados para resistir ataques cibernéticos. Le siguen el Reino Unido, Estados Unidos, Alemania, España y Francia. En el otro extremo, China, Brasil y México se encuentran entre los países con menos defensas para resistir una ofensiva[111].

Desde 2011, la Argentina también conformó un comando para defender al país de ataques cibernéticos y proteger las infraestructuras del sector público. El 28 de julio

de ese año, la Jefatura de Gabinete de Ministros dictó la resolución 508 por la cual creó el «Programa Nacional de Infraestructuras Críticas de la Información y Ciberseguridad[112]». Además de trabajar y capacitar a los organismos del Estado contra ataques, previene vulnerabilidades e implementar tecnologías de seguridad informática.

Si antes las guerras necesitaban dañar u ocupar un territorio, las rutas y las comunicaciones en un país o una ciudad determinada, hoy eso mismo puede hacerse a través de una o miles de computadoras puestas a trabajar en simultáneo, por ejemplo, atacando las computadoras de un organismo del ejército de un país enemigo o de una empresa con capitales de ese país. Todos los días leemos títulos que lo demuestran: «*Hackers* paquistaníes atacan la milicia india», «Apple sufrió el mayor ataque de su historia desde China», «Corea del Norte filtra documentos de una compañía norteamericana», «*Hackers* rusos atacan computadoras de la Otan», «Ciberejército iraní golpea Twitter».

Los ataques tienen orígenes muy diversos. Pueden provenir desde las propias cibermilicias oficiales hasta realizarse cuando distintos grupos de activistas de un país encaran un ataque contra una empresa o un objetivo en otro país. Muchas veces, los ciberejércitos oficiales también reciben ofensivas de parte de activistas virtuales de su propio país. Por eso, es necesario que cuando leamos «ataque de *hackers*» siempre pensemos que es un término que puede incluir dentro de sí expresiones muy distintas, que van desde hacktivistas más o menos organizados, hasta soldados financiados por un Estado y corporaciones. Ambos son *hackers* en el sentido amplio de la palabra: una persona que usa conocimientos de informática para penetrar una red. Pero los objetivos pueden ser sumamente diversos: desde el rechazo ideológico a una empresa extranjera, la venganza ante la actitud de una compañía o gobierno, la represalia por un acto puntual haciendo caer el sitio de una empresa, de un municipio o de la policía local. En general, la mayoría de los ataques son para desplomar un sitio o para filtrar una información, o ambas cosas al mismo tiempo. Uno de los procedimientos más sencillos consiste en que muchas computadoras, se pongan de acuerdo para lanzar ataques a un objetivo y colapsarlo. «El más común y más efectivo de los ataques, es el DDoS (ataque de denegación de servicio), el típico que hace que el servidor se sobrecargue y el sitio se caiga», me explicaba hace unos años un hacktivista que participa habitualmente de operaciones desde América Latina. Algunas organizaciones (como Anonymous) desarrollaron programas sencillos para bajarse de internet y sumarse a operaciones.

En una página adictiva de la empresa de seguridad informática Norse (map.ipviking.com) pueden seguirse los ciberataques del mundo, con origen y destino, y en tiempo real. La mayoría de ellos provienen de China, Rusia o algún país de América Latina y están destinados a algún blanco en Estados Unidos, en general a organismos de defensa (en Washington, Virginia, la costa este, o donde haya bases militares) o a compañías de internet (en general ubicadas en la costa oeste, alrededor

de Silicon Valley, aunque también pueden ser grandes compañías de telecomunicaciones como Verizon o AT&T, con sedes en distintas ciudades del país). Pero también ocurren desde Estados Unidos hacia, por supuesto, Rusia y China. Mientras escribo este párrafo, un domingo a la tarde, un día que debería ser tranquilo o de descanso, están ocurriendo 3854 ataques originados en China, 1447 desde Estados Unidos, 849 desde Rusia, 568 desde Alemania, 327 desde Japón, 319 desde Mil.gov (es decir, desde los dominios del ejército estadounidense), 289 desde Corea del Sur, 292 desde México, y el resto de la lista lo integran países de Asia y Europa. De todos los ataques, más de ocho mil están dirigidos a Estados Unidos. El segundo país es Rusia, que recibe menos de 300.

Corea del Norte es otro de los países con una cibermilicia poderosa, cuyas acciones llegan con frecuencia a la prensa internacional. El dato no es casual, ya que el país comunista, enemigo declarado de Estados Unidos, posee un porcentaje de personal militar enorme, de 40 soldados cada 1000 civiles. Su ciberejército ya cuenta con seis mil integrantes, en su mayoría jóvenes con habilidades de *hacking*, cuyo comando central, dependiente de Pyonyang, se ubica en la frontera vecina bajo el mando de Seúl. Dentro de ellos, hay un grupo de elite, la llamada «Oficina 121», que cuenta con 1800 jóvenes, seleccionados entre los mejores promedios de ciencias de la computación de la Universidad de Mirim y entrenados durante nueve años, en los que viajan a los países que atacarán, estudian su idioma y su cultura. Las cibermilicias de Corea del Norte realizan frecuentes ataques contra su vecino China, pero también contra objetivos de infraestructura de Corea del Sur como bancos, organismos militares, medios de comunicación y cadenas de televisión. Según expertos informáticos de todo el mundo, Pyonyang cuenta con algunos de los *hackers* más sofisticados del planeta. Sin embargo, y en una de las tantas paradojas de las guerras de internet, esto sucede en un país donde no existe el acceso a la web para la mayoría de la población. A diferencia de China, que tiene un gran firewall o barrera «alrededor» de su Red y donde sus ciudadanos pueden acceder básicamente a sitios con direcciones IP y contenidos provistos por empresas nacionales, en Corea del Norte solo existe el acceso para ciertos grupos restringidos, como funcionarios de gobierno y periodistas extranjeros. Esa es una de las razones por las cuales también es difícil penetrar en sus sistemas informáticos: al estar limitada internet a un ámbito cerrado es menos vulnerable a los ataques externos.

La ciencia ficción que hablaba de los juegos de guerra con enormes computadoras en la década de los 80, se volvió realidad. En internet ocurren y tendrán lugar en el futuro todo tipo de guerras, desde las estratégicas para robar datos sobre ventas de petróleo o filtrar cables diplomáticos sobre negociaciones de paz, hasta las pequeñas batallas de la cultura, los negocios y el entretenimiento. La razón es que la Red ya es otro terreno de la política internacional.

LA GUERRA POR LA PALABRA.
Libertad de expresión: medios, usuarios y el control de la opinión.

La segunda guerra se centra en internet como espacio de opinión. Los sitios, los blogs, los medios *online* y las redes sociales son nuevas plazas de expresión. En ellos comentamos, compartimos, calmamos nuestra sed de fama y ego subiendo una foto o compartiendo la de otros, y aplacamos la necesidad de que nos escuchen. La sensación de que estamos diciendo algo que muchos pueden leer es tan potente que también se hace adictiva: necesitamos decir lo que pensamos. Queremos que otros opinen, y opinar sobre lo que dicen los otros.

Con la masificación de las tecnologías, y en especial de internet, los costos de alcanzar audiencias son cada vez menores. También se amplió la posibilidad de que más personas, dominando algunas herramientas digitales sencillas, participen expresando su voz a través de blogs, medios digitales, redes sociales, o comentando la información ya disponible. Sin embargo, esto también produjo un exceso de información, que se multiplica exponencialmente todos los días. Para encontrar lo que queremos en ese caos se necesitan una serie de empresas que organizan, ordenan y filtran lo que los usuarios (que también son ciudadanos) buscan[113]. Ellos son los llamados intermediarios de internet, una serie (bastante grande y diversa) de organizaciones que van desde sitios de noticias, plataformas de blogs, redes sociales, buscadores, aplicaciones, sistemas operativos móviles, empresas que prestan conexión a internet o *hosting* (espacio de almacenamiento en servidores). Todos ellos son parte del intercambio diario de contenidos y opiniones, y, a medida que la Red contiene información de todo tipo, son también protagonistas de conflictos que es necesario dirimir.

¿Qué pasa cuando alguien sube, comenta o publica algo que afecta a otro? ¿Quién es responsable: el autor o la plataforma o empresa donde lo hace? ¿A quién y cómo deben responder los intermediarios ante un pedido de un gobierno, de la justicia, de otro usuario o de otra empresa? ¿Qué derechos tiene un usuario frente a ellos? La guerra está intrínsecamente relacionada con la libertad de expresión. Y los intermediarios son fundamentales porque, al mismo tiempo que son un nuevo espacio para volcar nuestras voces, son también dueños de un poder (que también buscan limitar otros poderes, por ejemplo, un gobierno).

Todos los días se producen reclamos para determinar si un contenido que pudo afectar a una persona tiene que ser eliminado de la Red o no. Las razones son diversas: algunas tienen que ver con la reputación o la intimidad, otras con dar de baja el resultado de un juicio que ya caducó o reclamar por derechos de autor. El tema es delicado porque por un lado está el derecho de una persona a que no se diga o se muestre algo que no quiera (por ejemplo, una foto de su intimidad o un dato de su pasado). Pero por otro está la libertad de expresión. La línea es finísima: intervenir

sobre los contenidos que se producen en internet puede coartar la libertad de expresión y caer en la censura, pública o privada. «Los intermediarios cumplen un rol esencial para ejercer el derecho de buscar y recibir información en línea», dice Eleonora Rabinovich, abogada de la Asociación por los Derechos Civiles[114]. Y explica: «La función de los intermediarios ha sido asociada frecuentemente a la de *gatekeepers*: actores privados que, por el rol que cumplen dentro de un contexto determinado, tienen poder para controlar o dirigir —en alguna medida— el flujo de las comunicaciones».

Esta guerra tiene nombre: la responsabilidad de intermediarios en internet. Y su pregunta clave es: ¿deben ser estos intermediarios responsables de lo que los usuarios hacen en la web? El conflicto es tan viejo como la expresión libre de la palabra, solo que ahora está mediada por una complejidad de actores y empresas a quienes confiamos diariamente los contenidos de la Red. Como Google, encargado de filtrar el mayor porcentaje de las búsquedas diarias de internet, o Facebook, donde cualquiera con una cuenta activa puede expresarse, subir comentarios, fotos, links. Todos los países, desde Estados Unidos hasta Europa y América Latina, están comenzando a enfrentarse con casos que involucran la responsabilidad de intermediarios y con jueces a los que se les solicita decidir sobre estos conflictos. Las sentencias, sin embargo, todavía no son unívocas y existen al menos tres caminos que los magistrados están tomando en la resolución de estos problemas.

El caso más conocido en Argentina sucedió cuando una modelo, Belén Rodríguez, demandó a Google y Yahoo por mostrar en los resultados de sus buscadores fotos donde se la vinculaba a sitios de pornografía, por lo que responsabilizó a ambas empresas por lesiones a su intimidad y honor. Luego de un extenso juicio que llegó hasta la Corte Suprema, el máximo tribunal emitió un fallo que establece que no puede condenarse a Google por lo que sucede en la web. En otros términos: no se puede condenar al bibliotecario por lo que dice el libro. En palabras de la Corte, no puede atribuirse una responsabilidad «objetiva» a los intermediarios de internet, como si ellos estuvieran comprometidos con cada contenido publicado en su plataforma. La razón es que si tuvieran esta responsabilidad tendrían que intervenir en los contenidos, lo que no es solo técnicamente complejo, sino que violaría otros derechos como la libertad de expresión y la privacidad (porque tendría que monitorearse previamente todo lo que se sube a la web).

Con su resolución, el máximo tribunal argentino tomó lo que Rabinovich denomina como una «tercera posición» respecto de los antecedentes que se vienen desarrollando en el tema en Europa y Estados Unidos. «En Estados Unidos, los intermediarios gozan de una cuasiinmunidad absoluta por los contenidos generados por terceros, pero cuando se trata de infracciones a los derechos de autor deben darlos de baja luego de una simple notificación de un particular», señala Rabinovich, en referencia al sistema conocido como *notice & takedown*, una forma rápida de

notificación y retiro extrajudicial que se adoptó en ese país por presiones de la industria del entretenimiento[115]. Sin embargo, el sistema tiene dos grandes riesgos en su funcionamiento. El primero, la eliminación excesiva de contenidos, ya que ante un solo pedido deben darse de baja. El segundo, que tales decisiones quedan en manos de unas pocas empresas que controlan el mayor porcentaje de las búsquedas *online*.

«En Europa, los intermediarios no son en general responsables salvo que hayan sido alertados sobre la actividad ilícita y no hayan actuado en consecuencia», explica la abogada, referente en el debate de los temas judiciales de internet en Argentina. El caso más comentado en Europa se resolvió en mayo de 2014 en España, cuando luego de seis años de litigio el abogado Mario Costeja logró que Google retirara de sus resultados de búsqueda enlaces que lo vinculaban con una deuda inmobiliaria de 1998, que aparecía en el diario *La Vanguardia*. Según ese medio, no se justificaba retirarlo porque era información legal. Pero Costeja entonces fue contra Google, a quien le reclamó que esos eran datos personales de una deuda ya saldada. La Audiencia Nacional de España finalmente le dio la razón, con lo que se generó el precedente del «derecho al olvido», es decir, que frente a un pedido efectuado ante el buscador por un ciudadano para dar de baja un contenido que lo relacione, Google debe dar curso a la petición. En 2014, el Tribunal de Justicia de la Unión Europea siguió el camino del derecho al olvido, declarando que las empresas que gestionan las búsquedas deben acceder a quitar los vínculos a páginas web de terceros que afecten a otra persona[116].

Sin embargo, los especialistas advierten sobre el peligro de que este tipo de decisiones queden directamente en manos de una empresa privada —en este caso, el megabuscador— a través de un simple formulario sin intervención de un juez o una instancia pública que defina el derecho que prevalece. En este punto, el tema es tan delicado como: ¿qué sucedería si quien pide la remoción de un dato es un político acusado de corrupción con una causa ya archivada, pero que luego de diez años se quiere presentar a elecciones? ¿No deberían los ciudadanos, por razones de derecho a la información, tener acceso a esos datos sobre las actividades pasadas de esa persona? ¿Quién determina dónde se pone un límite al pasado? Eduardo Bertoni, abogado y profesor de derechos digitales del Centro de Estudios sobre Libertad de Expresión de la Universidad de Palermo, advierte que, en el caso de los países de América Latina, con una historia de largas y crueles dictaduras, el derecho al olvido tendría serias consecuencias. Bertoni señala que sería un agravio para una región donde, «en lugar de imponer el olvido se ha estado peleando en las últimas décadas por la verdad de lo ocurrido durante los oscuros años de dictaduras militares. Búsqueda de la verdad y olvido son contradictorios». Como ejemplo, el académico destaca: «Si quienes estuvieron involucrados en violaciones masivas a los derechos humanos pudieran pedir, sin perjuicio del resultado de la solicitud, a un buscador de información en internet (Google, Yahoo, o el que se nos ocurra) que esa información

no sea posible de encontrar bajo argumentos, por ejemplo, de que es información extemporánea, resulta, por decirlo suavemente, un insulto a nuestra historia».

El derecho al olvido fue un concepto muy citado desde 2014, con optimismo de un derecho para los usuarios de internet. Sin embargo, tiene consecuencias, en tanto siempre es alguien quien decide. La respuesta no es sencilla. Como dice Bertoni, la solución quizá no sea restringir los contenidos, sino generar mecanismos para que más personas aún opinen sobre ellos, incluso denunciando los que no les gustan o infringen algún otro derecho.

También se ponen en conflicto nuevas soberanías. Al ser internet una herramienta global pero las decisiones tomadas por las justicias locales, ¿qué pasa si un país decide bloquear un contenido que afecta el derecho de otros países a verlo? ¿Qué derecho vale más? Es una cuestión de diseño tecnológico que afecta la palabra, pero también el conocimiento colectivo.

Pero para que internet siga siendo un espacio de libre opinión se necesitan otras condiciones, todavía no garantizadas para todos. La primera es el acceso. Los que tenemos capacidad económica, vivimos en ciudades con buen servicio, e incluso podemos elegir entre varios proveedores, lo damos por sentado. Pero no es todavía un servicio común para gran parte del mundo. En América Latina, cerca del 50 % de la población tiene acceso a internet, en el promedio regional. Sin embargo, en países como Haití, Ecuador, Honduras y Paraguay, el acceso llega recién al 10 % de la población[117]. Esta brecha digital, que no es más que una brecha social y económica, tiende a cerrarse paulatinamente, aunque todavía existen disparidades.

Pero además del acceso, una vez que «estamos» en internet necesitamos que nuestro derecho a expresarnos esté garantizado. El 5 de julio de 2012, el Consejo de Derechos Humanos de Naciones Unidas dictó una resolución donde declara que «los mismos derechos que las personas tienen fuera de internet deben ser protegidos cuando están conectadas». Es decir, que internet es otro espacio donde se ejercen, y también se tienen que defender, los derechos humanos. Y como todo espacio de derechos, también lo es de conflictos. La resolución de Naciones Unidas de 2012 se convirtió en una base para que las justicias nacionales tengan un marco legal para basar sus fallos, protegiendo a sus ciudadanos. «La relación entre derechos humanos e internet es compleja y no está exenta de matices. Si bien el acceso a internet ha potenciado la habilidad para ejercer la libertad de expresión, también es cierto que ha dificultado el ejercicio de otros derechos tales como el de la privacidad», explica Valeria Betancourt, activista ecuatoriana de derechos de internet[118].

Sin embargo, las guerras todavía son muchas, como denuncia la activista: «El bloqueo, control y manipulación de contenidos; el retiro de contenidos en línea por parte de proveedores de servicios sin un debido proceso; la interferencia con la privacidad y la protección de datos personales; la limitación de la calidad del acceso por parte de operadores y proveedores de servicios a fin de dar preferencia a ciertas aplicaciones y contenidos (por ejemplo, violando el principio de neutralidad de la

Red); la creciente presión por parte de los gobiernos sobre los intermediarios de internet para controlar el internet; la aplicación radical de la legislación de propiedad intelectual, entre otros aspectos, son prácticas cada vez más frecuentes y sofisticadas».

En cada país, los casos están en los medios todos los días: una celebridad o un ciudadano pide dar de baja un contenido, un legislador exige censurar a los sitios de noticias por «promover la discriminación», una empresa de entretenimientos intimida a un proveedor de internet a censurar sitios de descargas porque pueden afectar sus derechos de autor. El riesgo es que, en pos de proteger un derecho, limitemos otros. En internet esa línea es muy delicada y cada una de esas medidas suele ser desproporcionada según su objetivo inicial. Por ejemplo, para dar de baja una noticia a pedido de una celebridad, los buscadores suelen eliminar todos los resultados de una búsqueda de ese nombre. Eso fue lo que sucedió con Yahoo en Argentina, que suprimió todos los resultados relacionados con las modelos «Valeria+Mazza» o «Julieta+Prandi» para cumplir con órdenes judiciales. Por cuestiones técnicas, un pedido de un privado puede hacer que se borren partes enteras de internet, como sucedió cuando una corte de Pensilvania, Estados Unidos, encontró que un proveedor de servicios de internet borró cerca de 1,2 millones de sitios «inocentes» para responder a un pedido de agencias de seguridad para deshabilitar solo 400 sitios[119].

Algo similar sucedió el 30 de junio de 2014, cuando el juez argentino Gastón Polo Olivera ordenó bloquear el acceso desde Argentina a las direcciones IP y los nombres de dominio de *The Pirate Bay*, el sitio más conocido de búsqueda y descarga de *torrents*, a pedido de la industria de la música[120]. El magistrado argumentó que *The Pirate Bay* «facilita la violación de los derechos de propiedad» porque «el 25 % de los contenidos disponibles en el sitio se corresponde a música, de la cual al menos el 75 % está disponible para ser adquirida comercialmente». El problema es que el bloqueo se realizó para todo el sitio de descargas a partir de un pedido concreto. En pocas horas, la comunidad de usuarios reaccionó creando varias copias del sitio[121], que crecieron como cabezas de Hidra: ante cada baja se multiplicaban las páginas.

Pero no solo los jueces podrían decidir sobre qué podemos ver en internet. Desde sus distintas instancias, los gobiernos también lo hacen[122] con diversas medidas. Algunos limitando el acceso desde la infraestructura, con barreras para bloquear sitios o aplicaciones, o la salida de las conexiones hacia otros países. Otros, limitando los contenidos que pueden verse desde el país, con filtros o distintos tipos de censura a sitios o medios *online*, o usando internet para detectar activistas opositores y perseguirlos. Y también, violando los derechos a través de la vigilancia masiva y la intromisión en la privacidad. Entre los primeros países, los más conocidos por sus prácticas son China, Rusia, Cuba, Irán, Turquía, Ucrania y Angola. En términos de vigilancia, Estados Unidos es el país líder en este tipo de violaciones, pero no existe casi ningún gobierno (de Alemania a Brasil) en el mundo que no recurra a estas herramientas de intromisión para monitorear a sus ciudadanos, ya sea con la excusa

de la lucha contra el terrorismo, o de amenazas internas a la seguridad, o menos explícitas pero practicadas, como el espionaje político contra adversarios.

También existen propuestas de algunos legisladores que, intentando proteger ciertas libertades, atentan contra la libertad en la Red. En septiembre de 2014, el diputado argentino Remo Carlotto presentó un proyecto de ley donde proponía luchar contra la discriminación multando y clausurando sitios web con comentarios maliciosos. Entre ellos, incluía «páginas, blogs, redes sociales, agencias de noticias, medios de prensa, diarios *online*, revistas electrónicas y otros sitios de internet que admiten que los usuarios publiquen contenidos, opiniones o dejen mensajes en sus respectivos dominios». El problema de este proyecto es que delega a organismos especialmente creados facultades judiciales que ya existen en otras leyes. Es decir, que con un reclamo judicial podrían resolverse. Otros planes van más allá y proponen el riesgo de cerrar sitios completos para «prevenir» lo que algunos usuarios puedan expresar, lo cual es una medida claramente desproporcionada. Otro proyecto que generó polémica provino del diputado del PRO Sergio Bergman, que se sumaba a las entonces recientes iniciativas de derecho al olvido europeas proponiendo una ley que permitiera a empresas, organizaciones no gubernamentales y partidos políticos reclamar y obtener una rápida baja de contenidos por parte de los buscadores. El problema con estas ideas es que, ante un pedido de este tipo, las empresas siempre optan por dar de baja a una cantidad mayor de contenidos de los que son estrictamente necesarios.

Pero no solo es con leyes y la censura de sitios o contenidos como se puede afectar la libertad de internet. También hay conflictos que, partiendo de lo técnico, pueden implicar grandes riesgos a la forma en que hasta ahora la conocimos.

La guerra por la cultura. *Copyright: creación, monopolios y el control de la innovación.*

La cuarta guerra es quizá la primera que se presentó como tal —cronológicamente hablando— en la era digital. Se origina también en una posibilidad técnica que ofrece internet: la de copiar y distribuir contenidos de forma sencilla y barata, sin necesidad de dominar tecnologías complejas o costosas. Y enfrenta a quienes dominan la industria del entretenimiento con los millones de usuarios que gracias a las herramientas digitales pueden acceder a ellas más fácilmente. Pero además, pueden modificarlas, remixarlas y distribuirlas. Responde a una pregunta vieja que renació en la era de internet: ¿quién es el dueño de la cultura? O, más lejos: ¿de quién son las ideas que circulan en la Red? El gran inconveniente de esta guerra es que se presenta como un problema de internet en relación con el mundo del arte, la cultura o el

entretenimiento. Sin embargo, sus consecuencias afectan a toda internet, es decir, a ese espacio donde hacemos algo más que consumir entretenimientos.

En julio de 1999, Sean Parker y Shawn Fanning[123] crearon Napster[124], un programa que permitía compartir archivos de música en formato MP3. Fue la primera gran red de *peer-to-peer* (P2P), es decir, de intercambio de archivos entre usuarios de internet. Y fue un éxito. En los primeros nueve meses, Napster tenía 10 millones de usuarios registrados; dos años después, eran 26 millones. Sus inventores habían unido, por medio de un código, a la música que ya estaba disponible en la Red con gente que ya la compartía. Sin embargo, la industria discográfica cargó contra ellos rápidamente. En diciembre de 1999, los tribunales de Estados Unidos cerraron Napster por violación de derechos de autor. También vertiginosamente, aparecieron otros programas de intercambio de archivos P2P (Kazaa, Ares, eMule), demostrando que Napster simplemente funcionaba como un motor de búsqueda e intercambio de datos que ya estaban allí. Desde su creación, internet se trataba justamente de eso: de compartir información. El problema es que algunos —muy poderosos— no querían que sucediera. O, al menos, que no se hiciera sin pagarles.

Todo lo que existe en internet se puede tomar y modificar, y por lo tanto compartir. Como escribió el profesor de computación Lev Manovich en *El lenguaje de los nuevos medios de comunicación*[125], la característica fundamental de todos los objetos *online* es que son divisibles, combinables, capaces de variar. Esto es porque están hechos de pequeñas partes, los bits (caracteres de texto, música, imágenes), que podemos editar y combinar. Pero, además, lo que permite internet es la capacidad de distribuir los datos por nuestros propios medios. Antes, había que tener una imprenta, saber editar, tener máquinas costosas, dominar un circuito de distribución. Por eso la cultura circuló, desde Gutenberg hasta internet, dominada por monopolios, que también pusieron el precio a las obras, porque se encargaron al mismo tiempo de estipular y hacer cumplir los derechos de autor.

Con el nacimiento de la Red, la distribución está potencialmente en manos de mucha más gente. Con ello, la cultura, la música, el cine, el video, los libros, tuvieron una época dorada de creación. Pero entonces las corporaciones y la industria, que dominaron gran parte de la cultura durante siglos, empezaron a perder su monopolio. Como dice el escritor y ensayista italiano Alessandro Baricco en *Los bárbaros*[126], estos poderes se encontraron con «una revolución tecnológica que rompe de repente con los privilegios de la casta que ostentaba la primacía del arte».

Las grandes corporaciones no solo reclaman que se les pague por derechos de autor a quienes hagan circular «sus obras», sino también a quienes las exhiban, aunque no las hayan subido ellos mismos. Es decir, también inician demandas contra intermediarios de internet como YouTube, por ejemplo, por alojar un video o una canción (o partes de ellos) de su propiedad[127]. Por estos litigios, muchas veces un usuario de Argentina no puede escuchar canciones o ver videos cuyos derechos de autor no se negociaron localmente y entonces aparece una pantalla negra que nos

advierte que dichos contenidos «no están disponibles para la región» o «infringen derechos de autor».

La industria del entretenimiento, una de las más poderosas del *copyright*[128], declaró la guerra. Napster fue uno de los primeros capítulos. Los grandes estudios, las discográficas y las editoriales se enfrentaron a cualquier novedad tecnológica: apuntaron contra los programas de intercambio de música, contra los primeros reproductores de DVD alegando que se podrían copiar las películas, contra los libros y lectores de ebooks suponiendo que iban a terminar con los libros en papel, contra los servicios de películas por *streaming* que harían que nadie más fuera al cine. También limitaron, o directamente cooptaron, a las plataformas a través de las cuales se consume la cultura en internet, por ejemplo, servicios de video *online* como YouTube, con quien las discográficas y los estudios de cine y televisión realizaron acuerdos para que les pagasen por exhibir sus contenidos y para que estuvieran disponibles o no en ciertos países.

Esta industria está dominada por grandes corporaciones transnacionales y apoyada por artistas y autores locales, algunos muy enfáticos para reclamar sus derechos[129]. Las primeras patentes de propiedad intelectual las dictaron, en el Renacimiento, reyes que querían mantener para sí mismos el monopolio de lectura de ciertas obras. Trescientos años después, las grandes compañías de entretenimientos se basan en el mismo sistema porque su negocio principal es ganar dinero con las licencias de lo que compran y patentan. Entre ellas se encuentran las dos asociaciones más grandes: la Motion Picture Association of America (MPAA) y la Recording Industry Association of America (RIAA), que impulsaron, en octubre de 2011, la ley SOPA (Stop Online Piracy Act) ante el Congreso de Estados Unidos. En ese país, el paraíso de los *lobbies*, la ley SOPA proponía una pena máxima de cinco años de cárcel por cada diez canciones o películas descargadas. También que se bloqueara la financiación de sitios, sin probar delito, tal como le pasó a WikiLeaks cuando empresas como Visa o MasterCard le cortaron los fondos.

En Argentina, las guerras por el *copyright* y la cultura se dieron con otros casos muy resonados en la prensa, como los de Taringa, Cuevana y la plataforma colectiva de películas Popcorn Time (que recoge datos de intercambios de archivos *torrent*) y del sitio The Pirate Bay (sus direcciones IP locales). Los litigios fueron impulsados por la industria del entretenimiento y los autores locales, nucleados en Sadaic, Capif, Argentores y la Cámara Argentina del Libro. En el caso de Taringa, el segundo sitio de intercambio social más visitado de la Argentina después de Facebook, el 6 de mayo de 2011, la Cámara Nacional de Apelaciones en lo Criminal y Correccional envió a juicio a sus propietarios por supuesta infracción de derechos de autor, argumentando que eran «partícipes necesarios» por las acciones que realizan los usuarios dentro de la página, fundamentalmente el intercambio de libros y manuales de computación protegidos por derechos editoriales. Tras dos años de juicio, los querellantes decidieron retirar la demanda, declarando: «Internet debe mantenerse

como un espacio libre de censura, colocando el derecho a la libertad de expresión por sobre cualquier otro derecho social o económico». El portal de películas Cuevana también sufrió un cierre preventivo, en su caso por ofrecer series y películas de Warner, una de las empresas demandantes. Luego volvió a estar activo. Pero el debate siguió y continuará ante cada novedad que altere a la industria del entretenimiento[130].

La guerra del *copyright* fue la primera en dividir moralmente las aguas entre los «buenos y malos» de internet, que desde entonces fueron llamados despectivamente «piratas». Es también una de las guerras que ha tenido consecuencias fatales en la vida de algunas personas. Entre ellos, el programador y activista Aaron Swartz que, acusado por la justicia norteamericana por descargar documentos académicos, reseñas y publicaciones protegidas por leyes de derechos de autor de la base de datos JSTOR en el MIT, decidió terminar con su vida en enero de 2013. Swartz era un miembro destacado de la comunidad digital, no solo como militante de la cultura libre, sino como programador que había realizado contribuciones destacadas, como el desarrollo de la primera versión del código XML, que aún permite compartir contenidos en internet. Perseguido por una demanda desmesurada, señalado por pertenecer al lado «del mal», se suicidó a los 26 años.

También, en esta guerra, Gottfrid Svartholm, Fredrik Neij y Peter Sunde, los fundadores del sitio sueco de descarga de archivos *torrent* The Pirate Bay sufrieron consecuencias. Desde 2005, sus oficinas fueron allanadas, con la acusación de que allí se encontraba el centro de datos que alojaba contenidos ilegales (que estaban siendo compartidos por los usuarios). Luego de confiscar todos sus servidores, los tres administradores del sitio, que entonces tenían 22, 24 y 28 años, fueron arrestados y luego liberados. En protesta, 600 personas se manifestaron en las calles de Estocolmo y Gotemburgo. Al mes siguiente, el sitio estuvo de nuevo *online*. Pero en 2006 la justicia sueca inició un juicio en el que pidió un año de cárcel para los responsables de The Pirate Bay, acusados de piratería y violación a los derechos de autor. El tribunal los declaró culpables, les impuso un año de cárcel y una multa de casi un millón de dólares. Desde ese momento, el juicio continúa, con avances y retrocesos, los dueños del sitio continúan enfrentando detenciones y la página (y sus réplicas en el mundo) sigue siendo dada de baja periódicamente en distintos países (entre ellos Argentina) por violar derechos de autor.

La lucha entre los innovadores que lanzan al mercado nuevas tecnologías que habilitan la copia y los titulares de derechos de *copyright* es parte de una larga historia de tensiones que suma capítulos cada vez que las tecnologías corren límites[131]. El problema es que la historia del arte, la cultura, pero también de la innovación, siempre creció en base a desarrollos e ideas anteriores. Y a «los nuevos» siempre se los llamó piratas y se los acusó de piratería, es decir, de robar. Como

señala el abogado y activista de internet Lawrence Lessig: «Si la piratería significa usar la propiedad creativa de otros sin su permiso, si lo de "si hay valor, hay derecho" es verdad, entonces la historia de la industria de contenidos es una historia de piratería. Cada uno de los sectores importantes de los grandes medios hoy día (el cine, los discos, la radio y la televisión por cable) nació de una forma de piratería, si es que la definimos así[132]».

Un argumento en contra de la copia es que se trata de un robo. Pero es fácilmente rebatible: a diferencia de un libro o una película en sus versiones físicas, en el caso de internet, copiar y distribuir una obra no implica tener un objeto menos para vender. Por supuesto, no se trata de que los autores o creadores no reciban una compensación por su trabajo, ni de estar a favor del robo. Sin embargo, Lessig advierte que una cosa es proteger los derechos de los autores y otra dañar a toda internet para proteger a una industria[133].

La historia después de Napster comprobó dos cosas: que quienes usan las redes para intercambiar distintos tipos de obras también son quienes más consumen cultura, y que la industria también encuentra otras formas de financiamiento y pago para la música y las películas. La cultura siempre estuvo y estará sustentada en el conocimiento, de lo nuevo y de lo clásico. Si miramos en nuestros muros de Facebook, *timelines* de Twitter o cuentas conectadas a servicios de música como Spotify, gran parte de lo que compartimos son formas del arte. El entretenimiento tiene en internet su mejor socio. Ningún fenómeno masivo hoy lo es sin la ayuda de la Red, la primera ventana por donde los artistas o las grandes empresas de entretenimientos muestran sus productos, con campañas millonarias y hasta «filtraciones» (planeadas, por supuesto) de películas o discos antes de que se lancen oficialmente. Pero los mismos artistas tardan en comprenderlo. Neil Gaiman, uno de los escritores de ciencia ficción más vendidos del mundo, confesó: «Yo tenía la idea de que si subían mis cosas a la web me estaban pirateando. Hasta que me di cuenta de algo más importante: en los lugares donde los usuarios me pirateaban o traducían mis libros, vendía más. Porque me descubrían y querían comprar mi nuevo libro. Fue fascinante. Entonces puse mi libro *online* gratis por un mes. ¿Y saben lo que pasó? Las ventas aumentaron 300 %. Por eso, la otra pregunta que les hago a mis amigos es: ¿Cuánto de lo que descubriste y después compraste en los últimos cinco años fue porque lo viste en internet?».

Por otro lado, la industria de la música y del cine también idearon otras formas de venta *online*, algunas más independientes y otras haciendo acuerdos con compañías discográficas, con estudios de televisión o con artistas independientes. Lo demuestran los casos más que exitosos de Netflix y Spotify, que ya son grandes empresas en sí mismas.

Más que hacer un favor a los artistas, la guerra por controlar lo que se comparte en internet le produce un gran perjuicio a una parte mucho más grande de la gente: la que usa la Red. El escritor, periodista y activista Cory Doctorow lo explica: «No hay

una solución para el tema del *copyright online* sin que se dañe la salud de internet». Y argumenta: «Ser artista siempre fue un mal negocio. Estadísticamente, pueden vivir de ese trabajo unos pocos privilegiados, una fracción de 0,0000000000001 %. ¿Cuál es el verdadero problema? Que las guerras del *copyright* erosionaron la resistencia de internet en un tiempo en que la Red se necesita desesperadamente. Hoy internet está integrada en nuestras vidas de maneras que sobrepasaron hasta los pronósticos más salvajes de 1980. Es la forma a través de la que inscribimos a los chicos en la escuela, pagamos el gas, publicamos videos de violencia policial, le mandamos dinero a nuestros familiares, reservamos vacaciones, escribimos un trabajo para la escuela, nos ganamos la vida, hacemos las compras y todas las otras actividades de nuestra vida pública». Doctorow destaca que todas estas actividades de la vida diaria funcionan «dentro de internet», por lo tanto, ya no puede determinarse la libertad y el control por parte de empresas privadas, porque es un espacio público esencial de nuestras vidas. Su idea central es: no tiremos la bomba atómica para resolver un problema del tamaño de una hormiga. Porque la Red es más que entretenimiento. Es nuestra vida.

¿Cuál es entonces la solución para esta guerra? La respuesta de Doctorow es precisa, contundente: «La misma solución que necesitamos para la regulación de la prensa, para la guerra contra el terrorismo, para las guerras contra la vigilancia, para las guerras contra la pornografía: entender que internet es el sistema nervioso de la era de la información y que preservar su integridad y su libertad de la vigilancia, la censura y el control es el primer paso esencial para asegurarnos otras metas[134]».

La guerra de los datos.
Privacidad y vigilancia: huellas digitales, gobiernos y empresas.

La quinta guerra afecta nuestra privacidad. Su base es una combinación compleja de posibilidades técnicas, codicias económicas y la necesidad creciente de «seguridad» en un mundo a veces más amenazado o simplemente menos predecible. Su consecuencia es que estamos perdiendo, cediendo o dejando en manos de otros (empresas, gobiernos, otros usuarios) gran parte de nuestra información privada.

En el mundo hay 1,5 mil millones de computadoras y en 2014 se vendió ese mismo número de dispositivos móviles. Los aparatos son tan vitales en nuestra vida que ya no solo enloquecemos si nos olvidamos el celular al salir de nuestra casa: no podemos siquiera estar adentro de ella sin llevar la conexión con nosotros en todo momento. Vamos al baño con el celular, lo llevamos para ver videos o chatear desde la cama, *trackeamos* desde nuestro consumo de calorías hasta los kilómetros que caminamos en la semana, le preguntamos a Google en voz alta dónde queda tal negocio mientras vamos por la calle, dejamos registro de cada búsqueda, palabra e información en nuestros buscadores. Cada una de esas actividades va dejando una

huella. Debido a la arquitectura de internet, la información se copia muchas veces hasta llegar a su destino y pasa por muchos «lugares», donde van quedando partes de ella. Pero, al contrario de las migas de pan que dejan Hansel y Gretel para marcar su camino de vuelta, las huellas que dejamos *online* no son siempre voluntarias. Para preservar nuestros datos personales de terceros, buena parte de la información que circula en la Red está encriptada. Pero, aún así, hay otra que no lo está, otra a la que puede accederse igual, otra que cedemos voluntariamente y otra que simplemente no consentimos compartir pero que igual se comparte.

Las amenazas a la privacidad de nuestros datos provienen de distintos actores, con objetivos diversos, por lo que es casi imposible determinar un solo «responsable». El primer grupo de amenazas proviene de motivos económicos: las empresas que se valen de los datos que les dejamos voluntaria o involuntariamente en nuestro uso cotidiano, para luego vendernos cosas. El segundo grupo tiene que ver con el avance de la tecnología, a la que confiamos voluntariamente ciertos procesos para hacernos la vida más fácil: sería ridículo perder tiempo en ir a un negocio a comprar un producto si podemos tenerlo a un clic, hacer la fila para pagar un impuesto o hacer una transferencia si lo podemos hacer *online*, o perder dos horas para sacar un turno en una dependencia púbica si podemos resolverlo en un minuto en una página web; también, sería necio que si existen formas de comunicarnos con otras personas que están lejos a través de un programa sencillo lo evitemos, o que no usemos incluso algunos servicios de citas de internet si nos resultan una buena opción. El tercer grupo de amenazas se relaciona con la intromisión que realizan los Estados, ya sea porque realizan un espionaje abierto contra sus ciudadanos, porque cumplen con funciones legítimas pero a través de métodos que violan otros derechos, o porque eligen herramientas inadecuadas o excesivas para proteger la seguridad.

Cuando se habla de la pérdida de privacidad a causa de la tecnología, caemos en dos extremos. El primero es darle una confianza ciega como solución a todos los problemas. El segundo es temerle hasta la paranoia en su capacidad de entrometerse en nuestra vida. Sin embargo, ni internet ni la tecnología son —todavía— máquinas autogobernadas para actuar en contra de los humanos. Hay algo cierto: la pérdida de la privacidad es y será inevitable. Pero, antes de darnos por vencidos, es posible comprender en manos de quién están las responsabilidades y qué herramientas tenemos en nuestras manos como ciudadanos para defendernos. Porque en internet, además de consumidores, también podemos ser ciudadanos.

¿Ciudadanos o consumidores?

Internet creció en etapas y, con el tiempo, se sofisticó: permitió que los sitios tuvieran imágenes, audio, videos, contenidos interactivos. Con esto, la Red también se masificó y llegó a la vida cotidiana, con sitios de noticias, entretenimientos, luego

foros, blogs, clasificados y hasta redes sociales[135]. Pero con su avance, también necesitó construir un modelo de negocios, una forma de financiar ese gran mercado universal donde se crean y comparten contenidos. Ese modelo fue —y sigue siendo— la publicidad. Ese sustento económico fue también su riesgo futuro.

«Queríamos construir una herramienta fácil para todo el mundo, para compartir conocimientos, opiniones, ideas y fotos de gatitos lindos[136]», explica Ethan Zuckerman, profesor del MIT, activista de internet y exfundador de Tripod.com, una de las primeras (y entonces pocas) empresas exitosas de la llamada «burbuja puntocom[137]». Sin embargo, dice con autocrítica: con el tiempo las compañías de la Red necesitaron (y pudieron, gracias a la tecnología) recabar cada vez más información de los usuarios para «*targuetizar*» mejor los avisos. En otras palabras: si el *software* y los algoritmos le permiten a las empresas conocer cada movimiento de quienes visitan un sitio, cada clic que realizan, cómo navegan, qué temas, productos y servicios les interesan, lo van a usar en su beneficio, para generar una serie de ofertas acordes para cada consumidor y maximizar las posibilidades de venta. El modelo de las empresas es utilizar bases de datos cada vez más personalizadas con las preferencias de los usuarios, que les permiten ofrecer lo que cada persona quiere. Con exactitud científica y a un solo clic de esfuerzo.

Sin embargo, pasado el momento de la comodidad del consumo, el modelo de negocios de internet basado en la publicidad y la recolección permanente de datos pone en riesgo nuestra privacidad. Nos convierte en usuarios vigilados. Nos transforma en productos: valemos lo que valen nuestros datos, como dice la repetida frase «el producto sos vos» o «nada es gratis en internet, porque se paga con tus datos». El problema es que esos datos valen muy poco, comparados con los derechos que perdemos en el camino.

Para Zuckerman, este es el gran pecado original de la Red. ¿La razón? No hay forma de que una internet basada en la publicidad, en recabar crecientemente más datos de los usuarios para venderles productos y servicios, funcione sin niveles de vigilancia cada vez más detallados de cada acción de los usuarios. Los buscadores *online*, las redes sociales y los sitios de comercio electrónico crean herramientas progresivamente más sofisticadas para saber qué buscan, cliquean y compran cada segundo que están conectados. También sostienen departamentos de investigación y *Big data* que construyen perfiles minuciosos («*targets*») de los usuarios/consumidores. «La publicidad sin vigilancia es posible, pero es difícil de imaginar. Porque el principal beneficio de la publicidad *online* es la habilidad para ver quién está viendo un aviso», advierte Zuckerman.

Con el tiempo como usuarios y con la multiplicación de internet para todo tipo de operaciones y compras *online*, también nos vamos dando cuenta de cómo funciona este mecanismo de intercambiar comodidad y rapidez por privacidad. Sabemos, o al menos nos damos cuenta, de que cada clic que realizamos en una publicidad implica una ganancia para alguna empresa de la web o que nos llegan o vemos ofertas cada

vez más personalizadas para nuestro perfil de consumo. En cierto punto, sabemos que nuestras acciones están siendo «vistas» y «esperamos» que se nos vigile. Sin embargo, muchos todavía no son conscientes de cómo funcionan estos mecanismos y el cuidado de la privacidad todavía es una batalla perdida frente a la «comodidad» de usar la web tal como se nos presenta: dar aceptar a todas las condiciones de uso de sitios y dispositivos, navegar, buscar y comprar rápido y fácil, y olvidar (o más bien, ignorar a sabiendas) las consecuencias de nuestras acciones. El experto en seguridad informática finlandés Mikko Hypponen lo resume así: «Somos brutalmente honestos con nuestros motores de búsqueda. Somos más honestos con ellos que con nuestras familias. Los motores de búsqueda saben más de ti que tu familia[138]».

La investigadora norteamericana Rebecca MacKinnon explica este mecanismo de la era digital como «el consenso de los conectados», es decir, todos los problemas que preferimos no ver a cambio del «beneficio mayor» de utilizar las posibilidades de la web: comunicarnos, hacer amigos, comprar, opinar, apoyar una causa social o política, encontrar el amor, todo rápido con un clic. Para realizar cada una de esas acciones mudamos nuestra vida a plataformas digitales, servicios y dispositivos que hoy mediatizan todas nuestras relaciones. Y el problema, dice MacKinnon, es que esos espacios digitales van ganando un creciente poder, pero, al contrario del control que le reclamamos a otros espacios públicos de nuestras vidas (el barrio, la ciudad, el país, una escuela o un aeropuerto) todavía no nos ocupamos demasiado del poder que le damos a la nueva esfera *online*. «En nuestra dependencia, tenemos un problema: entendemos cómo funciona el poder en el mundo físico, pero todavía no tenemos un entendimiento claro de cómo funciona el poder en la esfera digital[139]», explica la académica. «La realidad es que las corporaciones y gobiernos que construyen, operan y gobiernan el ciberespacio no están siendo lo suficientemente responsables de su ejercicio de poder sobre las vidas y las identidades de la gente que usa las redes digitales. Hay soberanías operando sin el consenso de los que están conectados[140]».

En favor de los usuarios, en este caso también consumidores, ya existen (en cada país y en algunos continentes como Europa) leyes que van regulando el uso de los datos personales en internet y defendiendo a las personas de los abusos por parte de las empresas. La razón es que internet cada vez ocupa un espacio más grande en nuestra vida, como un nuevo espacio «público» donde todos interactuamos. Sin embargo, cada espacio de la web se rige por «leyes» de empresas privadas: los términos y las condiciones de las redes sociales o de los sitios de comercio electrónico, las fórmulas o los algoritmos de los buscadores (el *software*, o lo que está programado, también es una forma de ley que determina qué datos se retendrán de nosotros, por ejemplo), la forma en que operan las «*cookies*» (pequeñas piezas de información que sirven para identificar los rastros del usuario) en los sitios, entre otras leyes del ciberespacio. Como los usuarios también son ciudadanos, existen leyes de tratamiento de datos personales para regular su uso.

Un gran riesgo que deberá definir esta guerra es si el ecosistema de internet será cada vez más privado, al punto de que para conservar la intimidad debamos pagar. Algunos ya lo señalan: la privacidad, en el futuro, será un bien más de cambio, si no nos ocupamos hoy de que las leyes del mercado no la tomen en sus manos.

Ciudadanos espiados y controlados.

Las empresas no son las únicas que aprovechan la tecnología para intervenir en la vida de la gente. Los gobiernos —de países, pero también de ciudades de todo tamaño— también se valen de la interconexión total de nuestras vidas para espiar a sus ciudadanos y ejercer un control ya no solo de sus acciones, sino también de sus cuerpos. En efecto, el uso de la tecnología por parte de los gobiernos a veces se realiza con resultados positivos: ayuda a protegernos o está al servicio de procesos más eficientes, fáciles o rápidos en el Estado. Otras veces, la vigilancia o el espionaje son necesarios: para atrapar un asesino, un narcotraficante, evitar un abuso a un menor o el intento de poner una bomba en una escuela. Sin embargo, en otros casos, en nombre de vivir más seguros o modernizar nuestras vidas, se violan los derechos de los ciudadanos en el mundo digital.

No solemos pensarlo, pero en cada dispositivo que usamos o llevamos con nosotros, tenemos un arma de vigilancia. Los datos que circulan en los aparatos (cuando mandamos un *mail*, usamos una aplicación, hacemos una llamada, chateamos, publicamos una actualización en Facebook, una foto en Instagram o una frase en Twitter) pueden interceptarse, leerse y controlarse. Lo demostraron las revelaciones de Edward Snowden en 2013: desde Estados Unidos, la NSA accedía a la información de ciudadanos de todo el mundo. Lo hacía habilitada por su ley de seguridad nacional, que le permite espiar a los extranjeros cuando sus conexiones o datos entren en su país o pasen por él. El problema, como señala el informático Mikko Hypponen, «es que todos somos extranjeros, el 96 % del planeta es extranjero», porque las infraestructuras de internet pasan por el territorio de Estados Unidos.

Intervenir en «los cables», los «caños» o los datos es una de las formas de la vigilancia. Para hacerlo, se necesita de la cooperación de las empresas por donde circula la información, tal como Snowden demostró en su denuncia. Otra forma de lograrlo (la legal) es pedir a las compañías privadas que entreguen los dados de los usuarios con una orden legal. Pero eso no siempre sucede, como quedó demostrado en que la NSA y su par inglesa intervinieron también las redes privadas que conectan los centros de datos de Google y Yahoo en todo el mundo[141]. Quedó así claro que la intención no solo era buscar la información de casos puntuales que pusieran en riesgo la seguridad nacional, sino un mecanismo complejo de vigilancia generalizada y masiva, cuyas víctimas son todos los ciudadanos del mundo. La propia infraestructura

de la NSA lo demuestra: «El centro de datos de la NSA en Utah es cinco veces más grande que la tienda más extensa de muebles Ikea. Son 140 mil metros cuadrados que albergan supercomputadoras y *datacenters* que gastan decenas de millones de dólares al año en electricidad, capaces de guardar información prácticamente para siempre», señala Hypponen.

Cuando estalló el escándalo de la NSA, un comentario común fue «bueno, pero ya sabíamos que nos espiaban». Es cierto: suponíamos que sucedía. Pero tal vez lo más impactante fue confirmar la cooperación entre los gobiernos y las empresas con el objetivo de espiar. «Es como que se puedan meter en los códigos de las alarmas de todas las casas del mundo porque en algunas de las casas viven algunos tipos malos», explica Hypponen. Otro argumento fue que otros países también espiaban a su vez a Estados Unidos o a sus propios ciudadanos. También es cierto. «Pero la realidad es que no es equilibrado. Si Estados Unidos tiene derecho a espiar todas las comunicaciones que pasen por su territorio, entonces tiene derecho a espiar todo, porque todos de alguna forma usamos Windows, Skype, Dropbox, Linkedin, webmails y servicios en la nube. Si todos los servicios están en Estados Unidos, ellos tienen la ventaja de espiarnos. Los suecos usan los servicios de empresas estadounidenses, pero los estadounidenses no usan los servicios suecos».

El argumento que esgrime la NSA para defender sus operaciones es la lucha contra el terrorismo. Sin embargo, expertos y organismos internacionales advierten que, en nombre de combatir ese mal, se están violando otros derechos fundamentales, empezando por las convenciones de derechos humanos internacionales y las constituciones de cada país, que consagran el derecho a la privacidad como base de la democracia. En mayo de 2014, más de 400 de organizaciones del mundo presentaron los «Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones**[142]**», un documento que explica «cómo aplicar el derecho internacional de los derechos humanos en el actual entorno digital, en particular a la luz del aumento y de los cambios que están teniendo las tecnologías y técnicas de vigilancia de las comunicaciones». En el mismo, señalan que la intimidad es un derecho humano fundamental, porque si no estamos seguros de que no estamos siendo vigilados, es probable que no nos expresemos libremente, que no consultemos ciertos medios o que no nos reunamos con otras personas o protestemos contra algo que consideramos injusto. Por eso, la vigilancia de las comunicaciones solo se justifica cuando es prescrita por ley, es necesaria para lograr un objetivo legítimo y es proporcional al objetivo perseguido. Siempre debe precederse de estas preguntas: ¿existe una causa que justifique invadir la intimidad de esta persona**[143]**?, ¿es proporcional respecto de lo que se busca (por ejemplo: no es necesario espiar masivamente a todo un grupo ante la sospecha de un delito de una persona**[144]**?

Las organizaciones advirtieron además en su documento sobre el gran crecimiento no solo del espionaje, sino también de la información que guardan los Estados y los privados: «La frecuencia con la que los Estados procuran acceder tanto

al contenido de las comunicaciones como a los metadatos de las comunicaciones aumenta drásticamente, sin controles adecuados». El riesgo, escriben, es que esa gran cantidad de datos se conviertan en perfiles de los ciudadanos, «a partir de sus condiciones médicas, puntos de vista políticos y religiosos, asociaciones, interacciones e intereses, revelando tan o, incluso, más detalladamente de lo que sería posible desde el contenido de las comunicaciones».

A partir de este riesgo creciente, que se repite sin excepción en todos los países del mundo, los Estados también han ido dictando normas para proteger los datos personales de los ciudadanos. En la Argentina, la ley 25 326 de Protección de Datos Personales[145], sancionada en el año 2000, se encarga de proteger esta información asentada en archivos, registros, bancos de datos, públicos o privados, y cuenta con un órgano de control para hacer cumplir dicha ley: la Dirección Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia de la Nación. En la Ciudad Autónoma de Buenos Aires, desde 2005, existe una ley similar (la 1845[146]) y un organismo que se ocupa de tutelar a los vecinos en caso de violaciones a esta, el Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad de Buenos Aires[147]. Otros países, ciudades y regiones del mundo (como la Unión Europea) también cuentan con normas y organismos de defensa.

Sin embargo, muchas veces existe una «gobernanza» *de facto* por parte de las empresas a quien confiamos nuestros datos, que tienen sus propias leyes (términos y condiciones de uso) que los usuarios aceptan, quedando sus derechos en manos de esas legislaciones y tribunales que ni siquiera están en sus países. En ese punto volvemos al viejo problema: si la mayoría de los servicios web que utilizamos tienen su sede en empresas estadounidenses, estaremos finalmente sometidos a esa ley. Sin embargo, también hay antídotos que se pueden aplicar contra esa situación: usar programas de código abierto, seguros, comunicaciones encriptadas, tratar de salir de los servicios residentes en Estados Unidos. Es un camino que requiere informarse, leer los términos y las condiciones con los que se maneja nuestra información y aprender ciertas herramientas técnicas. En síntesis: demanda que entendamos más la tecnología. Pero, hoy, si no lo hacemos, estaremos dejando nuestras vidas digitales en manos de otros; será como no haber leído la Constitución o como no comprender cuáles son nuestros derechos.

En los países de América Latina, además del terrorismo, existe otra excusa para intervenir en la intimidad de los ciudadanos: la inseguridad. Para combatir esta amenaza, los gobiernos de todo signo político están invirtiendo presupuestos millonarios en armarse con cámaras y centros de operaciones donde pueden ver, en tiempo real, qué hacen sus ciudadanos. Repletos de camaritas, funcionan las 24 horas como Ministerios de la Verdad, como panópticos de ciudades que se pueblan con ojos electrónicos que no vemos, aunque sabemos que están. Pero las imágenes no solo son

usadas por los gobiernos, sino que también son fuente de horas interminables de materiales para noticieros y canales de televisión que usan lo que se capta en la vía pública para mostrarlo a quien quiera verlo. De esa forma, el círculo de los medios que muestran ciudades inseguras se retroalimenta con ciudadanos que demandan más seguridad y Estados que entonces llenan los techos con cámaras, porque «la gente lo pide». El problema es que esas imágenes no siempre son tratadas con los requisitos legales y de respeto de derechos humanos establecidos por los tratados internacionales que la mayoría de los países deberían cumplir.

Quedan cada vez menos espacios libres en las ciudades sin vigilar. Basta con mirar hacia arriba en cualquier calle y ver cómo las cámaras nos filman. Las instalan las ciudades, los gobiernos nacionales o municipales. Lo hacen sin preguntar, alentados por el «reclamo ciudadano» de más seguridad. Si vivimos en Buenos Aires, los porteños convivimos con más tres mil cámaras distribuidas en distintos barrios, es decir, una cámara cada mil habitantes. En el resto del país, cada provincia y municipio avanza con sus propios programas de vigilancia. También lo hacen los sistemas privados, con circuitos cerrados de televisión en *shoppings* y edificios, y en una creciente cantidad de espacios públicos como plazas, escuelas, hospitales y aeropuertos. Sin embargo, todavía no existen estadísticas que confirmen que vivir rodeados de cámaras reduzca efectivamente el delito en general.

En ese intercambio, también vamos perdiendo privacidad. Muchas veces, incluso, lo aceptamos. Otras veces, también somos responsables, cuando la tecnología nos convierte en policías del otro: queremos saber a qué hora se conectó, qué foto subió, con quién habló. Como escribe Julian Assange: «No solo vivimos en un estado de vigilancia; también vivimos en una sociedad de vigilancia. La vigilancia totalitaria no está solo encarnada en nuestros gobiernos; está incrustada en nuestra economía, en nuestros usos mundanos de la tecnología, en nuestras interacciones diarias[148]». La naturaleza misma de internet y la tecnología permite la vigilancia. Por eso, prestarle atención a la privacidad es relevante.

«Yo no tengo nada que esconder»: ese es un argumento común de quienes no se preocupan por la privacidad o de quienes honestamente no sienten que tienen que protegerla. También lo utilizan las empresas o gobiernos para justificar sus prácticas de vigilancia diciendo que solo observan a quienes cometen delitos. Pero, si la información no tuviera ningún valor, ¿por qué es tan importante para empresas como Google o para los gobiernos? La razón es que sí es valiosa, ya sea con objetivos comerciales o con otros relacionados a la vigilancia estatal. En *Nada que esconder. El falso intercambio entre privacidad y seguridad*[149], el profesor de derecho de la Universidad de Washington Daniel Solove señala que ese argumento es el más utilizado, justamente, por quienes violan la privacidad. Supone que si no hicimos nada malo no deberíamos temer, con lo cual nos supone previamente culpables y nos genera una culpa si no admitimos «cooperar» con quienes quieren «saber» sobre nosotros.

Solove ofrece varios argumentos para responder contra esa presión. El primero: «¿Por qué deberíamos justificar cada acto previamente? Yo no tengo nada que justificar. En todo caso, si tienen algo que me incrimine, vuelvan con una orden judicial». El segundo: «No tengo nada que esconder, pero tampoco tengo nada que quiera compartir con usted». El tercero: «Si no tenés nada que esconder, entonces no tenés una vida». El cuarto: «Mostrame lo tuyo, entonces te muestro lo mío». El quinto: «No se trata de tener algo que esconder, sino de no formar parte del negocio de otro». Solove dice que las razones podrían seguir hasta el infinito, porque la privacidad es tan compleja que está en cada acción de nuestras vidas. Si no, no tendríamos cortinas en las ventanas, iríamos desnudos por la calle o no nos molestaría que alguien lea nuestros *mails*. Pero la verdad es que si eso nos sucede, nos enojamos. Que la tecnología esconda la vigilancia no significa que ella no exista. O, como dice otra frase famosa: «Que yo no sea paranoico no significa que no me estén vigilando».

Los argumentos anteriores tienen que ver con lo individual. Pero la privacidad también es un derecho colectivo. Y allí reside otra de sus dimensiones más importantes. Incluso cuando no nos preocupe mantener nuestra intimidad, ella tiene un valor fundamental para la democracia. Como decíamos, es un valor en sí, porque permite la libertad, desde el pensamiento hasta la protesta. Nos permite ser iguales, al menos para expresarnos. Por eso, cada vez que admitimos dejarla en manos o no pedir su debido control a empresas o a gobiernos, también estamos dañando la libertad de toda la sociedad. Si hoy no nos importa que se espíen las comunicaciones de un político o un periodista con el que no acordamos, permitirlo también es abrir la posibilidad de que mañana se espíe a cualquier otro, incluidos nosotros. Si mañana hay un golpe de Estado o nuestro país se convierte en una dictadura, y no defendemos hoy nuestra privacidad, cualquier parte de nuestra información puede ser utilizada para encarcelarnos, porque sí, porque a alguien no le gustó lo que dijimos. Ese es el riesgo de la «justicia selectiva»: todos tenemos información que puede ser usada en nuestra contra. Aún más los activistas políticos, los periodistas, o cualquier ciudadano que participe en la vida pública.

Ante estos riesgos, todavía estamos a tiempo de protegernos, de cuidar y reclamar nuestra privacidad, y de pedir a gobiernos y empresas que la respeten. Para eso, primero es necesario conocer quiénes y cómo nos vigilan, cómo nos espían y qué hacen con nuestros datos.

Cuarta parte

De las cámaras de seguridad a tu celular: Cómo la tecnología te controla (aunque no te avisen).

VIII

Vigilar y entretener, un modelo de negocios feliz

> «Espiar a todo el mundo puede no atrapar terroristas, pero sí hace que los contratistas militares y las empresas de telecomunicaciones ganen mucho dinero. La vigilancia masiva es política con un modelo de negocios».
>
> CORY DOCTOROW.

> «Si no hay derecho a la privacidad, no puede haber verdadera libertad de expresión y de opinión, y entonces no puede haber una democracia efectiva».
>
> DILMA ROUSSEFF.
> Asamblea General de la ONU, 24 de septiembre de 2014.

—¿Vas acá, a las cámaras, no?

El taxista deja de silbar por un momento la zamba *El arriero* y se asegura de haber interpretado bien el destino. Llegando al Centro de Operaciones Tigre (COT), por la ruta provincial 24, asoma un clásico paisaje del conurbano bonaerense: a cada lado del camino la gente espera el colectivo, en fila, bajo el sol; otros, en bicicleta, hacen las compras en los negocios del barrio. En El Talar, la segunda localidad más poblada de Tigre, las calles del norte se mezclan con los arroyos que desprende el río Luján. Desde el sur, el río Reconquista recuerda que la seguridad de la ciudad siempre dependerá del humor de sus aguas submarinas.

Nos acercamos a un edificio de 4500 metros cuadrados, vidrios negros, marquesina roja y un felino (el logo de Tigre) que lo custodia desde el techo. Para los vecinos, el COT es «el lugar de las cámaras». En la ruta del camino hay caballos, casas sin terminar, piletas Pelopincho en las puertas y chicos jugando con tachos de pintura convertidos en baldes de agua. El barrio está igual que hace 30 años. Pero, apenas cruzando el portón de la gran construcción, lo primero que se distingue en el COT es una camioneta hipertecnológica. Preparada para combatir y prevenir delitos, tiene pantallas de plasma, conexión satelital a internet, un mástil con una cámara domo y un dron preparado para actuar. En el mismo playón de acceso, antes de ingresar, un grupo de los 42 móviles de la policía local descansa de su turno. Están

equipados con GPS, cámaras que filman hacia adelante y hacia atrás, hacia adentro y hacia afuera, y un sistema que graba lo que se dice en el vehículo.

Cruzando el acceso, colmado de seguridad, pasamos los molinetes y llegamos a una segunda entrada. «Solo personal autorizado», dice el cartel de la puerta que conduce al espacio más grande: la sala de monitoreo. Allí, las 24 horas de los 365 días del año, 300 empleados miran, controlan y alertan sobre los movimientos que registran las 1300 cámaras que custodian los 360 kilómetros cuadrados del partido.

En la pared central, 18 monitores registran cada movimiento del municipio: los peatones que cruzan la avenida hacia el puerto fluvial[150], la gente que se baja en la última estación del tren Mitre, los grupitos de chicos en las esquinas, los novios que se besan tímidamente en los bancos de las plazas, las mamás que vuelven con sus hijos de la escuela en moto en los barrios más humildes. A cada lado, los cien operadores del turno tarde miran sus pantallas. Adentro, un aire acondicionado glacial los mantiene despiertos en una tarde de calor. Del otro lado del vidrio, un patio poblado por plantas de hojas grandes y árboles recuerda que la naturaleza todavía existe, a pesar de su aislamiento, aunque adentro la luz de las imágenes que cambian varias veces por minuto solo muestra un mundo artificial.

Un continuado de alertas visuales y auditivas distrae la atención; pero el silencio humano gobierna. No se escucha ni un murmullo. Los operadores no hablan entre sí. No está permitido, excepto que los supervisores les pregunten por una imagen en particular. La tarea requiere que permanezcan inmóviles, callados, como si estuvieran encadenados con grilletes al escritorio asignado. Solo deben abrir los ojos y estar atentos para detectar posibles problemas. Son *voyeurs* profesionales de la vida de los otros en el panóptico de esta ciudad del conurbano.

Durante 40 minutos, la función de cada operador es mantener los sentidos atentos, detectar cualquier movimiento sospechoso o confirmar con la vista una denuncia que llegó por teléfono. Después, descansar 20 minutos en una sala de relax, con mesas de ping pong y biblioteca, o salir al espacio verde, fuera del aire acondicionado y las luces de artificiales. En esa tregua, tienen permitido mirar sus celulares, recordar sus vidas hablando con sus novios, sus maridos, sus hijos. Cumplida la pausa, hay que volver al puesto. Así sucede durante toda la jornada laboral. Cuando vuelven a ingresar a la sala de monitoreo no pueden llevar ningún elemento electrónico con ellos: no hay celulares, ni reproductores de música ni cámaras. Nada que pueda registrar lo que allí sucede. Sus caras y sus cuerpos también están resguardados: todos visten chombas negras y unas gorras con viseras anchas.

—Tenemos que protegerlos. Ellos también viven en un barrio.

La supervisora del turno me explica por qué cuidan tanto la identidad de los operadores. Son en su mayoría jóvenes, repartidos casi por igual entre hombres y mujeres que ingresaron al trabajo bajo el requisito de tener el colegio primario completo y conocimientos de informática. Luego, la exigencia fundamental es estar

concentrados. Mucho. El trabajo de operador de cámaras de seguridad es permanecer fiel a un monitor, para que nada de lo que sucede en el mundo exterior se escape.

Una de las operadoras, una chica que no llega a los 30 años, se distingue del resto: está muy maquillada, con las uñas perfectas pintadas de azul, el pelo recogido en un peinado de verano con pequeñas hebillas de colores. Cuando la observo en su tarea, detrás de su silla, levanta un momento la vista y me saluda girando levemente su cara para que pueda encontrar su sonrisa. Al instante, vuelve a su monitor. Le devuelvo la sonrisa: sé que no la llegó a ver, pero que la distingue. Sus sentidos están acostumbrados a mirar por fuera de los límites de su cuerpo. Sabe que además de observar está siendo observada. Conoce las capas de una realidad que ya casi nunca es privada: ella mira, otros la miran, yo la miro a ella. Y seguramente desde algún lado alguien también me mira.

Del otro lado de la sala, otro operador vuelve de su descanso. Mientras se ajusta la gorra del uniforme, acomoda su cuerpo enorme en la silla y deja en el escritorio una Coca-Cola recién abierta que será su compañía en su nuevo turno. Él no parece registrar otro mundo más allá de las fronteras de su cubículo. Aquí es un robot humano que permanece quieto hasta encontrar algo extraño en su monitor.

Cuando concluyen sus turnos, los operadores dejan de ser quienes miran a sus vecinos desde la pantalla durante ocho horas y regresan a sus barrios. Allí se convierten otra vez en ciudadanos comunes, observados y controlados también por las cámaras. Tal vez, por deformación profesional, ya no piensen que sus vidas transcurren como antes: sin que nadie los mire. Quizás se olviden, en algún momento, de que están siendo observados. Pero seguramente ya intuyen que no son tan libres.

El Centro de Operaciones Tigre, inaugurado en 2008, hoy también es la sede de la Secretaría de Protección Ciudadana del partido y donde se desempeñan también empleados de la Dirección de Tránsito y Transporte, Defensa Civil y de la Dirección de Derechos Humanos, que se encarga del control de las funciones de seguridad. En la estructura del ministerio, los 300 operadores de cámaras son el grupo más numeroso. Son quienes trabajan en el sector más visible, el de videovigilancia, el sistema implementado en 2008 cuando el entonces intendente y actual diputado provincial Sergio Massa instaló los primeros ojos del monitoreo urbano. Hoy, siete años después, las cámaras ya son famosas. Son casi sinónimo de Tigre y se replican en otros municipios a través de la televisión que las muestra protagonistas de operativos varias veces por semana. También, son la imagen misma del futuro: para Massa, hoy candidato presidencial de la Argentina[151], la seguridad es el principal eje de campaña, e instalar cámaras, ahora en todo el país, una de las primeras medidas que su gobierno tomaría si llegara al poder.

—Cuando Sergio visita una villa, no le piden un plan social. Le piden que instale cámaras.

Santiago García Vázquez tiene 37 años y hace diez trabaja en el equipo de prensa de Sergio Massa. Es alto, habla fuerte y rápido: parece que en su mente las decisiones se toman al instante o que ya tiene todo tan pensado desde antes, que cuando actúa solo está ejecutando un plan. «Distinto a ellos, igual a vos. La Argentina que viene», le dicta a una periodista que lo llama para pedirle novedades de la campaña. «Vamos a salir con ese eslogan», aclara y se acomoda en un sillón de cuero de diseño retro, en una oficina del edificio Torre de las Naciones, un monstruo de vidrios espejados azules a 200 metros de la estación del tren Mitre en Tigre. Su jefe es uno de los tres candidatos que más miden en las encuestas para convertirse en el próximo presidente argentino. Él, que fue parte de su camino desde el inicio, está orgulloso. Se jacta de la estrategia de medios que ejecutó junto al jefe de prensa histórico de Massa, Claudio Ambrosino. En ella —dice Santiago— la presencia mediática diaria, basada en la lucha contra la inseguridad, los condujo al éxito.

—A Sergio lo identifican con las cámaras de seguridad —me dice—. Las cámaras atrapan delincuentes. Por lo tanto, hacen justicia. Y Massa está preocupado por la seguridad. Es la primera vez que la seguridad se identifica como algo positivo. Por eso la gente lo ve y le pide cámaras. Y por eso pudo ganar un espacio de poder.

—*¿No es peligroso «usar» la inseguridad para hacer campaña*? —le pregunto.

—Yo tengo el desafío de instalar a Massa como presidente. Pero Massa es uno más de los 135 intendentes de Buenos Aires. ¿Por qué un medio de comunicación nacional va a estar interesado en algo local? Es muy difícil. Entonces nosotros comunicamos seguridad. Y necesitamos mostrarlo. Yo, desde hace siete años, tengo que lograr que dos veces por semana «las cámaras de seguridad de Tigre» salgan en los medios.

—*Si el objetivo era ese, lo lograste. Las cámaras de Tigre están en todos lados*.

—Claro que sí. Te digo más: nosotros hicimos que las cámaras sean protagonistas. «Las cámaras permitieron atrapar un delincuente», «Las cámaras lograron tal cosa», «Las cámaras tal, tal y tal». Queríamos publicitar las cámaras y lo logramos. Al final, Tigre también redujo un 80 % el robo de autos. Pero nos llevó siete años de trabajo.

—*Los medios fueron fundamentales. ¿En qué momento los convertiste en aliados de las cámaras?*

—En 2010, durante un viaje de Sergio, me llamaron del COT. «Se cayó una avioneta en la ruta 197 y Colectora, al lado de una estación de servicio». Podía haber explotado todo, pero los pibes de las cámaras la vieron a tiempo: mandaron a los bomberos en minutos y no estalló nada. La cámara era espectacular: vos veías al avión caer, *bruuuuum*. Buscalo hoy en YouTube y tiene miles de visitas. Era buenísimo para la televisión. Los productores de los noticieros mataban por tener eso.

—*¿Y qué hiciste*?

—Me estallaba el teléfono, tenía a todos los productores quemándome la oreja: «Dame la cámara, dame la cámara». Entonces hablé con Sergio. «Si vamos a dárselas a los medios, tiene que ser una estrategia de aquí en adelante», me dijo. «Pero que cuenten que gracias a las cámaras se pudo prevenir una emergencia. Que digan que dan resultados». Y así fue. Les mandé la grabación de la cámara a todos los canales, por moto. Ahora ya avanzamos tanto que directamente subimos las cámaras a un servidor para que las bajen, todos al mismo tiempo. Somos muy democráticos con eso. Y también, obviamente, a veces tenemos que pedir autorización a la Justicia para difundir algunas cámaras. Pero siempre se las damos a los medios.

—*Pero la decisión fue cuestionada en ese momento. No todos estaban de acuerdo con darle ese material a los medios*.

—Obvio. Los sectores del viejo peronismo de Tigre cuestionaron por qué hacíamos prensa con las cámaras. ¿Sabés por qué? Porque fuimos los primeros. No había centros de monitoreo y una política tan agresiva de comunicación. Yo tenía un video donde caía una avioneta y llegaba una ambulancia en seis minutos. Ni siquiera tenía que editarlo. ¡Todo en tiempo real! Para los canales era una papa caliente.

—*Y sobre el tema de la privacidad de las imágenes, ¿tuvieron resistencia, debates?*

—Sí, porque todavía no éramos tan fuertes políticamente. En el Concejo Deliberante todavía gobernaba la oposición que se resistía a aprobar presupuesto para la fibra óptica de las cámaras con el argumento de la privacidad. «Es meterse con cosas delicadas, es hacer *marketing*, no política», decían. También se resistían en nuestro propio bloque. Pero Sergio estaba decidido: «Vamos a fondo con esto», decía. Al final, ganamos, pusimos la fibra óptica y las cámaras empezaron a funcionar.

—*Para vos, si las cámaras funcionan, el debate no es tan importante*.

—Mirá, toda la comunidad «más intelectual» plantea el debate privacidad/cámaras. Pero la realidad es que el robo de autos bajó. Yo no ingreso con una cámara a la propiedad privada. Si se cae un avión en un *country*, como ha pasado, y yo tengo al avión en el cielo, eso lo puedo mostrar, es mío. Yo no muestro nada de adentro, pero mientras cae no es propiedad privada, ¿no?

—*Pero vos, personalmente, ¿te planteaste si era bueno vivir rodeado de tantas cámaras?*

—Sí, a mí me hacía ruido el tema. «¿Qué onda si hay personas dándose un beso en un auto o están en un departamento y el pibe que está monitoreando es un perversito?», decía. Pero hay un protocolo de acción para los operadores que les impide invadir la privacidad ajena. Si eso sucede, se los separa del cargo. Y hasta

ahora nunca sucedió. Yo se lo tuve que explicar mucho a los periodistas. La cámara previene. Tenemos cámaras con escuchas donde los chorros dicen «Mejor no vayamos a Tigre porque filman» o «No vendamos droga acá». Se disuade a los delincuentes para que no elijan Tigre.

—*Justamente, una de las críticas a los sistemas de videovigilancia es que previenen el delito en un territorio, pero lo corrés a otro lugar. Se va al partido lindero, a San Fernando, por ejemplo.*

—Está bien, pero ahí lo que Massa plantea es que él tiene una responsabilidad con los vecinos de Tigre que lo votaron a él. Él necesitaba que Tigre fuera seguro. Después, podrás trabajar con San Fernando para que tampoco estén allá. La idea es correr a los tipos. En definitiva, que no estén acá. Ahora que quiere gobernar el país, también lo plantea: una cámara cada mil habitantes. Sergio lo dijo siempre muy claro: cuantos más ojos tengamos, mejor. Cuanto más vigilado esté el territorio, mejor.

—*Entonces la solución a la inseguridad es llenar el país de cámaras. Hasta que los delincuentes se caigan al río, por ejemplo.*

—Bueno, hay lanchas del COT en el río.

Santiago García Vázquez sonríe. Pero habla en serio. Repite lo que su jefe declara en los medios: «Argentina necesita una cámara cada mil habitantes. Cuantos más ojos vigilando tengamos, más seguros estaremos». Para Massa, la seguridad se trata de introducir la tecnología a la vida de la gente. En su Argentina del futuro cada movimiento puede verse y atacarse.

Massa**[152]**, de 43 años, no es el único político argentino ni del mundo que recurre a las cámaras como una solución eficiente contra la inseguridad. Pero sí fue el primero en presentarlas como el eje de su plan. Su país perfecto está vigilado con un «cerrojo digital» donde no pueden entrar los delincuentes, donde queden del lado de adentro los ciudadanos «de bien». Si son delincuentes, no son ciudadanos. Tigre, el lugar que gobernó y donde hoy vive, es su ejemplo a copiar y extender al resto del país.

Los 380 mil tigrenses ya son parte del experimento: conviven con una cámara cada 290 habitantes, un número que se incrementa año a año, y un modelo que se contagia a los distritos vecinos como San Fernando o Escobar, que también se van armando de tecnología. Es una ciudad-Gran Hermano, donde vivir siendo visto es el precio a pagar por sentirse seguro. Tal vez el éxito del famoso *reality show* que encierra a un grupo de jóvenes conscientes de ser filmados, que alcanzó popularidad en Argentina en 2001, en el año de una de las peores crisis del país, haya preparado culturalmente a la sociedad para la realidad que hoy aceptamos.

En el norte de Buenos Aires están algunas de las ciudades más vigiladas de la Argentina. También, las más fragmentadas: en Tigre hay un 60 % de territorios ocupados por *countries*, barrios cerrados y complejos urbanos de altos ingresos. Allí

vive solo el 10 % de la población de Tigre (y el propio Massa, que vive en el barrio cerrado Isla del Sol). El 90 % de la gente vive en el 40 % restante del municipio. El 91 % de las viviendas cuenta con buenas condiciones de habitabilidad. Sin embargo, todavía hay un 47 % de hogares sin gas y el 83 % aún no tiene cloacas[153]. Pero, según el candidato del Frente Renovador, lo que los vecinos reclaman es más seguridad. Por lo tanto, más tecnología.

Desde su llegada al poder en Tigre, la seguridad fue uno de los ejes de campaña de Massa. Su estrategia, tanto para la seguridad como para otros aspectos de la gestión pública, incluye una gran dosis tecnológica. En su municipio, los patrulleros, los colectivos, los bancos, los boliches bailables también tienen cámaras, sistemas de GPS y botones de pánico conectados al Centro de Operaciones de Tigre, el mismo lugar donde llegan y se vigilan las imágenes de las 1300 cámaras (en su mayoría modelo domo). Los ingresos y egresos del partido también fueron poblados de fibra óptica para permanecer vigilados. Las patentes de los autos que cruzan los límites de municipio son monitoreadas por cámaras especiales. En las cuatro estaciones (de tren, el puerto fluvial y las dos terminales de ómnibus) también hay instaladas cámaras especiales fijas, que trabajan con reconocimiento facial, en áreas de gran circulación de personas, especialmente durante el fin de semana. Además de recurrir al sistema provincial de alertas 911, Tigre también cuenta con Alerta Tigre 2.0, un sistema que funciona vía SMS y alerta a su policía local ante delitos. Las mujeres víctimas de violencia de género son provistas de un dispositivo de alerta especial. El municipio también posee tres drones y con pilotos especialmente capacitados que cumplen guardias en caso de que se necesite utilizarlos.

La tecnología también está presente en los distintos procesos del Estado a través de una oficina de innovación donde funcionan unas 15 áreas que se valen de tecnología para brindar servicios a los ciudadanos. Allí se gestiona desde el manejo de las redes sociales hasta las señales de tránsito informatizadas y la actualización de todos los sistemas de información y alerta del municipio: las entradas y salidas de la autopista, el tránsito, el nivel del río, las alertas y posibles crecidas del agua en las islas. La ayuda social y los servicios a los vecinos también están informatizados. Sin embargo, lo que el candidato Massa hace más visible es la tecnología aplicada a la lucha contra la inseguridad. Según él, es la muestra de que invertir en tecnología genera resultados positivos para la sociedad. Son, como él también dice, una muestra de «gestión».

Sergio Massa —como sus otros compañeros de la generación política intermedia[154], Mauricio Macri, Daniel Scioli, Francisco De Narváez o Jorge Capitanich— ama la gestión. Si para las generaciones políticas anteriores (la primera, de Antonio Cafiero y Raúl Anfonsín, que gobernó la primera democracia; la segunda, la generación del 70, siguió con Cristina y Néstor Kirchner, Elisa Carrió, Hermes Binner) la ideología estaba en la base del discurso y la acción que los llevó al poder, para Massa y sus contemporáneos se trata de hablar «desde afuera de la política».

Ante el «fracaso de la vieja política», suelen decir, hay que llegar a la gente desde el sentido común. Las ideas (o la ideología) no son relevantes (aunque todos, sin excepción, se dicen peronistas). Lo importante es hacer. Es la gestión. Es mostrar resultados. El periodista Martín Rodríguez los describe de esta manera: «El talismán de los intermedios es la palabra *gestión*, una palabra que no tiene dicción de izquierda y que vincula su pasión pública a la idea de hacer, ya que ese hacer también habilita su exposición. Pone *los hechos* por encima de *las palabras*».

La gestión es tiempo. Es hacer las cosas rápido, sin pasarlas por el tamiz de la ideología. No se necesitan cuadros académicos o intelectuales —como tenía la izquierda—, sino «planes estratégicos» creados por «equipos técnicos». De allí a la incorporación de la tecnología como herramienta destacada de la gestión hay un paso. La tecnología tampoco tiene —para ellos— política ni ideología. Es un medio para conseguir resultados. Se compra, se usa y ofrece una solución. Como una licuadora, una plancha o cualquier electrodoméstico, su función es hacer lo que le corresponde. Si además lo hacen rápido, mejor. Porque la gestión tiene en los medios de comunicación su gran aliado. Lo que no se puede mostrar en imágenes no existe. Lo que no se puede comprobar rápidamente, tampoco. Si la cámara atrapó a un ladrón de estéreo esta tarde, la imagen tiene que llegar a la pantalla esta misma noche.

Pero además de rápido y para los medios, gobernar con «gestión» se trata de hacerlo con alegría, bajo una forma descontracturada y «natural». Tan alejada del conflicto que parece una política sin manchas de realidad. Como dice el filósofo esloveno Slavoj Žižek, es la ilusión de que se puede obtener lo que se quiere sin sufrir[155]: tomar cerveza sin alcohol, Coca-Cola sin azúcar o café descafeinado, formas de obtener placer sin pagar a cambio ningún costo. Llevada a la política, es la idea de que puede haber un capitalismo sin pobres. Llevada a la tecnología, la idea se vuelve todavía más poderosa. El ejemplo más rotundo de la ilusión está en los drones, los vehículos artillados no tripulados, símbolos de la guerra del siglo XXI, que permiten matar sin morir.

Si en los países del norte del mundo o en las potencias más poderosas se trata de utilizar la tecnología para combatir al gran enemigo-terrorismo, en América Latina la gran amenaza es la inseguridad urbana. Para derrotarla también se compran y se utilizan aparatos y tecnologías: cámaras de seguridad, drones, sistemas biométricos de control de personas.

Mientras los cuerpos están cada vez más vigilados, los datos que registran los aparatos van quedando en manos de distintas autoridades de gobierno y seguridad. Nuestra privacidad, además, queda en poder de las empresas que proveen las tecnologías y que gestionan las bases de datos. En ellas, hay información tan sensible que permite identificar por sus huellas digitales o el iris de su ojo a una persona o acceder con un clic a las imágenes de los lugares que transitó: una estación de tren, una calle, un colectivo, una ruta. Sin embargo, esa información no siempre es tratada con la seguridad que corresponde. A veces simplemente se utiliza como un insumo

más para lograr resultados «de gestión». Con esos «resultados» se ganan elecciones o al menos se los publicita para ese fin. En el camino, la tecnología se sigue instalando en todas las ciudades del país. Sin debate público sobre sus usos, sobre los presupuestos que se destinan a comprarla o sobre quiénes serán los dueños de los datos y cómo los manejarán. Simplemente, se multiplican entre nuestros cuerpos y los espacios que ocupamos.

Tigre es uno de los distritos más vigilados por cámaras de seguridad en la Argentina. Pero sus 1300 cámaras no están distribuidas por igual en toda la localidad: en los *countries* no hay cámaras públicas. Eso implica que el resto del municipio, las 152 mil personas que viven «muros afuera», es decir, en los barrios de menos poder económico, es la zona más vigilada. En Tigre la mayoría de las cámaras son modelo «domo», una especie de ojo oscuro en forma de esfera insertado adentro de una carcasa que permite mirar en 360 grados hacia distintos puntos sin que se pueda divisar fácilmente hacia dónde está apuntando. La marca más común, tanto en ese distrito como en el resto del país, es Bosch cuyo modelo VG4 y VG5 es el más comprado por las ciudades argentinas. Las cámaras, importadas, se adquieren a través de licitaciones, que —también, en un gran porcentaje del país— son ganadas por Global View, la empresa líder del mercado, que además de vender las cámaras provee su mantenimiento y las conecta con las redes de fibra óptica para transmitir sus datos. Junto con el modelo domo, tanto en Tigre como en otras localidades, también se utilizan otros modelos de cámaras, fijas, direccionadas a ciertos puntos, por ejemplo para detección facial en zonas muy transitadas, como estaciones de tren o terminales de colectivos. En estos casos, se utilizan cámaras Panasonic con tecnología DVR (son un circuito cerrado, que graba imágenes en forma analógica, que luego son digitalizadas).

En la Ciudad Autónoma de Buenos Aires (CABA), sus 3 millones de habitantes conviven con 3200 cámaras. O sea, hay una cada 930 personas. Las primeras se instalaron en 2005 en la Plaza Houssay, entre la Facultad de Ciencias Económicas y de Medicina de la Universidad de Buenos Aires, durante el mandato del entonces jefe de Gobierno porteño Jorge Telerman. En 2007 se creó el primer centro de monitoreo de la ciudad y se cubrieron las plazas públicas con 74 cámaras. En 2009, con la puesta en marcha de la Policía Metropolitana (la fuerza local), se extendió la vigilancia. Hoy, existen 2000 cámaras, que se suman a las 1200 instaladas también en suelo porteño por la Policía Federal.

Un porteño, un visitante de la ciudad o un turista que camina por la Avenida 9 de Julio desde Independencia hasta Santa Fe será filmado doce veces, si se cuentan solo las cámaras oficiales (y se omiten las de empresas privadas). Las plazas, avenidas y lugares con mayor tránsito de personas (el Obelisco, las estaciones de Retiro y de Once) son las que tienen más presencia de cámaras. Entre los barrios, Puerto Madero

se destaca como el más vigilado, si se considera que para los solo 8000 habitantes de sus 2 kilómetros cuadrados se emplean 25 cámaras: es decir, una cada 300 habitantes, una cifra cercana al promedio de Tigre. El vecindario tiene una tasa bajísima de ocupación: solo el 28 % de sus residencias están habitadas. Pero recibe todos los días 45 mil turistas de alto poder adquisitivo, que además de las cámaras policiales son registrados por la gran cantidad de cámaras de los edificios desocupados y por la Prefectura, que mantiene en la zona una tasa de delito cercana a cero. En el resto de la ciudad sí se registran delitos. Se concentran en otras zonas de alto poder adquisitivo: Palermo, Recoleta, Belgrano, Núñez y Colegiales.

La Policía Metropolitana tiene un Centro de Monitoreo Urbano (CMU) en su sede de Barracas[156], sobre la Avenida Patricios. Allí, en el sur de la ciudad, en el sexto piso de un edificio rodeado de construcciones modernas, convive un equipo de cinco programadores de *software* que se encargan de las tareas técnicas, un equipo de legales que procesa los pedidos judiciales que llegan para las imágenes[157] y los empleados civiles y policiales que trabajan en dos salas.

En la primera, más pequeña y oscura, se reciben las alertas de los botones de pánico instalados en edificios públicos, centros de jubilados, clubes, inmobiliarias, comercios, iglesias y templos religiosos, y los que se reparten a encargados de edificios, testigos protegidos en causas judiciales y mujeres que sufren situaciones de violencia de género, entre otros. Decenas de monitores resaltan en la oscuridad, muestran mapas de los barrios e imágenes de colores según las alertas.

En la segunda sala, más luminosa, con una vista que se abre hacia el este trabajan 30 operadores en tres turnos de ocho horas, con quince minutos de descanso por cada 60 minutos de monitoreo de imágenes. Las edades son muy variables y van desde jóvenes que no llegan a los 30 años hasta otros mayores de 50.

Distribuidos en tres filas de escritorios, los operadores se ubican de frente a una gran pantalla conformada por 12 monitores que muestran un paneo de toda la ciudad. A las once de la mañana de un miércoles, con mate, café y un ventanal chorreado de una lluvia ventosa de verano, los empleados civiles de la Metropolitana acercan y alejan el mouse y eligen distintas tomas de las cámaras. Cada operador ve 16 cámaras durante su turno. Solo acerca el *zoom* de la cámara ante un «escalamiento», que en la jerga policial implica un movimiento extraño, una salida de humo o un movimiento excepcional. Si eso sucede, avisa al oficial superior y allí puede acercar más la cámara a un punto determinado (la puerta de una casa, un balcón, el banco de una plaza o una persona). En caso de confirmarse un delito o una situación que requiera de acción, el oficial le avisa al comando del Centro Único de Coordinación y Control, ubicado al norte de la ciudad, en un edificio de la calle Guzmán, en Chacarita, que se encarga de enviar un patrullero, una ambulancia o lo que requiera el caso.

El inspector Jorge Brieva, hoy a cargo del CMU, trabaja hace 24 años en el área técnica de la policía. Primero se desempeñó en telecomunicaciones de la Federal y ahora se encarga de las cámaras de la Metropolitana.

—Nuestra fuerza ya nació digital, pero los que atravesamos la experiencia analógica también la volcamos acá —cuenta—. Podés tener las cámaras, pero siempre estás atento y tenés que capacitarte en cómo cambia el delito. Los que tenemos muchos años detectamos un movimiento sospechoso apenas sale en el monitor.

Flaco, camisa y corbata impecables, afeitado y peinado como si fueran las ocho de la mañana, Brieva explica que, además de las cámaras, la Metropolitana cuenta con otras herramientas tecnológicas dedicadas a la seguridad: un camión de exteriores similar al de los canales de televisión (con dos cámaras domo y dos fijas), dos «mochilas de rápido despliegue» que transmiten imágenes en 3G y un dron propio[158]. Desarrollado por la propia Policía durante dos años, el llamado «Metrocóptero» se utiliza para el control del tránsito y para sobrevolar zonas durante situaciones de emergencia[159].

En la tercera fila de escritorios de la sala de monitoreo de la Metropolitana se encuentran los supervisores desde una tarima, que ven la gran pantalla de 12 monitores y también las de todos los operadores. En el escritorio principal, una pantalla les muestra, en vivo, las principales cadenas de noticias porteñas: TN, C5N, Canal 26, CN23 y los canales de aire 13, 11, 9, 7. En algunos canales, las cámaras son protagonistas, mostrando los movimientos de tránsito de la mañana. En la siguiente señal televisiva, las imágenes ocupan la programación con un robo frustrado o un choque la noche anterior. En otra emisora, un *talk show* transcurre entre sus noticias de chimentos, la receta de pionono de atún y el móvil desde Mar de Plata. Al igual que para otros gobiernos, para el de la ciudad de Buenos Aires mostrar «gestión de seguridad» a través de las cámaras también es prioritario.

—¿*Cuán importante es para su área la relación con los medios*? —le pregunto al inspector Brieva.

—Es importante. Nos interesa que la sociedad sepa lo que está pasando. Y también ser fuente de información de los medios. Por ejemplo, cuando difundimos el caso de los limpiavidrios que robaban en la Avenida 9 de Julio queríamos alertar a la gente y que supieran que sabemos que eso ocurre. Sin la prensa no se vería lo que hacemos.

—¿*Los vecinos siempre aceptan la presencia de las cámaras*?

—Casi siempre. En algunos asentamientos no y cuando rompen las cámaras por vandalismo tampoco. En esos casos, nuestra policía acompaña a las empresas que instalan las cámaras y las esperan con los móviles durante la instalación.

En la Metropolitana, una vez que las cámaras toman las imágenes, las guardan en una base de datos durante 60 días para que las autoridades judiciales cuenten con ese material de prueba para sus causas. Pero también existen casos donde ciudadanos hacen pedidos específicos o los seguros las piden como documento, por ejemplo, en el caso de un choque.

Además de Tigre y la ciudad de Buenos Aires, otras ciudades del país, en especial las de mayor densidad de población, también se están proveyendo de cámaras de videovigilancia. Según datos del Ministerio de Seguridad de la Nación, en los 135 municipios de la provincia de Buenos Aires hay nueve mil cámaras activas y 125 centros de monitoreo[160].

Los municipios del norte de la provincia —entre ellos varios controlados por el massismo y el PRO— están entre los primeros lugares. San Isidro, con 1030 cámaras para 45 mil habitantes, tiene un alto promedio: una cada 45 habitantes, conectadas por 100 kilómetros de fibra óptica y monitoreadas desde la una sala de control ubicada en el mismo edificio de la Municipalidad. En Vicente López se instalaron 400 cámaras, para 270 mil habitantes: una cada 675 personas.

En el centro del conurbano bonaerense, el partido más habitado es La Matanza, con 1,8 millones de personas registradas por 600 cámaras. Está lejos de las cifras de Tigre o San Isidro. Si sus habitantes quisieran llegar a los promedios de los vecinos del norte, tendrían que convivir con 6000 cámaras, diez veces más que las actuales (que además serían imposibles de monitorear). Con diferencias en cantidad y etapas de avance quedan pocos de los 135 municipios sin comprar cámaras y expandir las redes de fibra óptica para conectarlas. Cada cámara cuesta entre 15 y 30 mil pesos, según sus prestaciones. El presupuesto para hacerse de ellas y tender las redes de fibra se realiza en muchos casos con recursos locales del partido, y en otros con dinero de programas de seguridad de la provincia o de la nación. Cuando los municipios tienen gestiones opositoras a la del gobernador, las compras de tecnología para seguridad se suelen publicitar más y se las vincula con una «preocupación» de los intendentes para «ocuparse de la seguridad de los vecinos» mientras «otros no se ocupan» (en este caso, el Ejecutivo provincial).

No solo se publicita la compra de cámaras, patrulleros «inteligentes» y botones de pánico. También se muestran las capacitaciones a los policías y a los operadores que se encargarán de monitorear las imágenes, de mirar a los vecinos para mantenerlos seguros. En las redes sociales de los municipios, los vecinos agradecen y también reclaman tener su cámara, en su cuadra, para vigilar su casa: «Quiero una cámara en 202 y Sobremonte, gracias», dice Cecilia en el Facebook del municipio de San Fernando. «Se necesita una cámara en la esquina de Ambrosoni y Alem (Victoria) todas las noches se juntan a tomar alcohol y fumar porro, ni hablar de que venden drogas», escribe su vecina Florencia. «Ocúpense del barrio Mil Viviendas. Pongan cámaras. ¡Hay mucha delincuencia, señor intendente!», pide Bárbara. «Que pongan una cámara en la calle Beltrán y Miguel Cané, que todos los fin de semana se matan las barras de niños y niñas a piedrazos y botellazos, ¡parecen cavernícolas!», se queja Claudio.

Sergio Massa, en Tigre, no es el único que invirtió en su entramado tecnológico para la seguridad, pero fue uno de los primeros que se animó a promocionarlo y

defenderlo de sus detractores. Pero también respaldaron el modelo de las cámaras las máximas autoridades de la provincia. Apenas designado en su cargo de ministro de Seguridad en 2013, el exintendente de Ezeiza Alejandro Granados dijo que había que instalar «miles y miles y miles de cámaras» para enfrentar la inseguridad y que había que «llenar la provincia de policías y cámaras».

Como en la película *Minority Report* o en la serie *Person of Interest*, los funcionarios defienden los sistemas omnipresentes que todo lo ven para anticipar lo malo. Les gusta saber que pueden trazar el camino de las amenazas para esperarlas antes de que lleguen. Si lo hacen las películas, ¿por qué no lo pueden hacer ellos? La tecnología es cada vez más barata, está disponible, no requiere enormes inversiones de instalación. Una cámara de seguridad sale menos que un televisor de última tecnología. Un operador cobra un sueldo básico de empleado municipal y no requiere una formación compleja: con saber computación y seguir un protocolo de acción es suficiente.

La misma presidenta de la Argentina, Cristina Fernández de Kirchner, se pronunció a favor de la videovigilancia: «Yo quiero camaritas en todas partes», dijo el 3 de diciembre de 2012 durante la inauguración de un sistema de escaneo en el Puerto de Buenos Aires[161]. «Mientras más cámaras pongamos, mejor», repitió varias veces durante el acto, en el que recordó cómo los ojos electrónicos habían permitido encontrar al narcotraficante Henry de Jesús López Londoño, alias «Mi Sangre», que se había refugiado en Argentina[162]. La Presidenta fue consecuente con su voluntad. Desde marzo de 2009, el Gobierno nacional destina partidas presupuestarias extraordinarias para financiar el Plan de Protección Ciudadana, que permitió al gobernador y candidato a presidente Daniel Scioli desplegar la compra de cámaras y tecnología para luchar contra el delito en la provincia de Buenos Aires.

Las cámaras, por ahora, son una buena solución para todos: para los gobiernos, una forma de mostrar gestión en seguridad, un reclamo de las encuestas y los medios. Para los vecinos, tener más cámaras significa sentirse más protegidos. Entonces los presupuestos para comprarlas aumentan. La provincia de Buenos Aires está planificando que los municipios con menos presupuesto, que aún no compraron cámaras, o que tienen buena relación con el poder central, lo hagan: Tres de Febrero, Esteban Echeverría, Berazategui se suman a la lista. En el verano de 2015, Mar del Plata inauguró un centro de monitoreo que su intendente, Gustavo Pulti (del Frente para la Victoria), publicitó como «el más grande de la Argentina», con inversión en sistemas de acceso biométrico y facial, y sala de servidores propia. La videovigilancia se acrecienta en tiempos electorales y se convierte en también en una forma de competencia entre los municipios para ver quién construye el búnker-panóptico más grande.

Las ciudades pequeñas no escapan a la lógica. En el interior más profundo de la provincia de Buenos Aires, asociadas popularmente a la calma rural, donde no existe el delito y la gente puede «dormir con la puerta abierta», también se inauguró la

carrera tecnológica. En Carlos Casares, la ciudad cabecera de una localidad agropecuaria de 22 mil habitantes, ya hay instaladas 20 cámaras, un centro de monitoreo y la proyección de instalar 20 más. En esa localidad, sede de la Fiesta Nacional del Girasol, los vecinos también donan cámaras al municipio que los medios locales reflejan con orgullo.

En el resto del país el panorama es similar. Las grandes capitales de las provincias también incorporan cámaras. En Córdoba hay instaladas 150 cámaras, en Santa Fe 400, 100 más en el municipio de Rosario y otras 600 previstas para colocar. En Río Negro, las ciudades de General Roca y Cipolletti tienen 200 cámaras. San Luis cuenta con 500 cámaras de seguridad para un territorio de 500 mil habitantes, publicitadas como «un elemento diferenciador a la hora de ser elegida por los empresarios para invertir». Paradójicamente, esa misma provincia se jacta de tener algunos de los paraísos turísticos del país como Villa Mercedes y Merlo, donde hoy también se están instalando de cámaras. Algo similar ocurre en Tafí Viejo, en la provincia de Tucumán, una localidad de 39 mil habitantes, Capital Nacional del Limón. Allí se instalaron 125 cámaras, una cada 300 habitantes, y se instaló un centro de monitoreo con tecnología comprada a Movilnet, una empresa de Ushuaia, en el otro extremo del país.

En el mundo, el avance de la videovigilancia se incrementó a partir de 2001, luego del atentado a las Torres Gemelas en Nueva York, y los ataques terroristas en Madrid y Londres en 2004 y 2005. En Estados Unidos y Europa, la «amenaza terrorista» fue y continúa siendo el argumento utilizado para incrementar el control urbano. En América Latina, la excusa que justifica el avance de la videovigilancia es «la inseguridad».

Brasil tiene dos de las ciudades más vigiladas del mundo: San Pablo y Río de Janeiro. Entre las cámaras estatales y las privadas, en la capital financiera del país se calcula que existe una cámara cada 8 habitantes, un número que inquieta frente al promedio de una cada 14 personas de Londres y de una cada 36 habitantes en Beijing, dos de las ciudades más vigiladas del planeta. En todo el Reino Unido hay 5,9 millones de cámaras, entre las públicas y las privadas. En Estados Unidos, Chicago lidera el *ranking* con 22 mil cámaras, una cada 127 habitantes. Nueva York, que recibe 40 millones de turistas al año y en donde viven 8 millones de personas, solo tiene 5 mil cámaras.

El avance de la videovigilancia es sostenido y omnipresente. Pero instalar cada vez más ojos no es una solución sustentable, porque es casi imposible para los ojos de los humanos monitorear todas las imágenes que suceden en una ciudad. Se necesitaría otra ciudad paralela, imaginariamente construida en los subsuelos de la ciudad real, para vigilar todo lo que sucede arriba, en sus calles. Con robots (¿o tal vez con las mismas ratas que hoy son plaga en las profundidades de las urbes?) se podría llegar a

ese ideal de una persona siguiendo a otra persona para prevenir que cometa algún delito. Pero la tecnología tiene una solución más eficiente: ahora que las cámaras son *commodities* que ya todos tienen se están desarrollando tecnologías que interactúen con ellas para volverlas más «inteligentes». La tecnología ya tiene nuevas cámaras inteligentes, que están sumando programas que no solo filman, sino que también reconocen caras, miran patrones de movimientos, reacciones inesperadas de una persona o que detectan sensorialmente (con temperatura o ruidos) si se están concentrando grupos de personas en una esquina o en una calle (potencialmente, pueden ser un grupo de amigos yendo a bailar, o un grupo de manifestantes con bombas).

Pocos países, entre ellos Canadá, se resisten a la tendencia creciente de la videovigilancia. En el país del norte de América, el avance de las cámaras todavía es lento y se topa con fuertes debates respecto del tratamiento de las imágenes y la privacidad de los ciudadanos. Es uno de los pocos lugares del mundo donde —aun cuando las cámaras pueden traer beneficios, por ejemplo, para la prevención de algunos delitos— se está produciendo un debate público sobre la verdadera relación costo-beneficio de adoptar el sistema, antes llenar de ojos las calles.

La tentación de comprar soluciones técnicas envasadas es tan grande que se evitan algunas preguntas y debates importantes. ¿Hasta dónde armarnos de cámaras resuelve el problema de la inseguridad? ¿Siempre gastar más implica bajar el delito, o se necesitan otras soluciones? ¿Qué consecuencias sociales y culturales estamos dispuestos a tolerar a cambio de ser monitoreados permanentemente? Finalmente, una última pregunta políticamente central: ¿quién decide la incorporación de tecnologías: el Estado o el mercado? ¿La decisión se basa en demandas y estadísticas reales o en las campañas de *marketing* de las empresas de tecnología?

La incorporación de cámaras no está relacionada con los índices de criminalidad. Antes que en las estadísticas, los gobiernos las incorporan por decisiones que toman por ellos las fuerzas del mercado. Los negocios privados son los que deciden que nos estemos armando de cámaras sin preguntarnos para qué, cómo se usan, cuánto pagamos por ellas (en dinero y en bienes no materiales como libertad y privacidad). Aunque no es algo nuevo: las guerras impulsadas por las corporaciones de defensa y vendedores de armas, las epidemias y sus lazos con las grandes multinacionales de patentes de medicamentos o los virus de las computadoras cuya solución está en grandes corporaciones tecnológicas son otros ejemplos.

En Argentina y en el mundo la instalación de las cámaras no responde a criterios racionales. La compra de tecnologías de videovigilancia no se debe a criterios demográficos: hay grandes urbes con pocas cámaras y ciudades pequeñas con cientos de cámaras. Tampoco se basa en las estadísticas de los delitos: además de ser difíciles de conseguir, los censos de inseguridad se basan en distintos parámetros (denuncias policiales que siempre son incompletas, datos del sistema de salud, información de compañías de seguros, estadísticas privadas y del Estado) y miden delitos muy

diversos. Sin embargo, cualquiera de ellos también parece resolverse con cámaras. Existen ciudades con altas tasas de delitos urbanos que trabajan con planes extensos de instalación de cámaras, pero también distritos con pocos delitos que compran ese tipo de equipamiento. Hay ciudades donde se roban autos, otras donde el crimen más común es producto del narcotráfico y otras donde la seguridad urbana crece para prevenir las consecuencias de la desigualdad social. Pero ante situaciones de inseguridad tan diversas, la tecnología se presenta como una solución común. No solo eso: en todas las ciudades —más allá de su trama de delito distinta— se instalan los mismos modelos y marcas de cámaras, y las venden los mismos proveedores. «Bosch», «Panasonic», «cámaras domo de 360 grados» son palabras que pueden repetirse en una licitación de Tafí Viejo, Tucumán, y Chicago, Estados Unidos. También en Tucumán o Chicago se reproduce la ilusión de que tener un iPhone es estar mejor comunicado con el mundo. O que guardar nuestros datos en manos de Google es más seguro que hacerlo en una carpeta de nuestra computadora o en un *pendrive* de 20 dólares comprado en el supermercado. El *marketing* de la tecnología, el «furor por lo nuevo», nos lleva a instalar cámaras como solución mágica contra la inseguridad. El fetichismo, por ahora, le gana a las estadísticas.

Todavía no hay datos contundentes que demuestren la relación efectiva entre instalar cámaras y reducir el delito. Incluso los promotores más entusiastas —con poder económico para publicitar la tecnología en los grandes— aún no se animan a realizar afirmaciones elocuentes. En febrero de 2015 la revista británica *The Economist* realizó el informe «Ciudades seguras**[163]**», cuya investigación estuvo financiada por la empresa de tecnología japonesa NEC, uno de los mayores proveedores mundiales de tecnología de vigilancia y control biométrico para gobiernos del mundo**[164]**. Ni siquiera este trabajo, un claro producto del *marketing* para publicitar sus ventajas en cada ámbito de la vida urbana, afirma que la seguridad es solo consecuencia de la tecnología. En cambio, junto con las virtudes de las ciudades inteligentes, destaca que los factores de desarrollo humano y la reducción de la desigualdad social siguen siendo tan importantes como siempre para vivir seguros. Es decir: la tecnología puede ser «linda» (y puede incluso funcionar como un placebo para hacer que nos sintamos protegidos), pero nunca es determinante por sí sola para reducir la inseguridad si no está acompañada por otras mejoras en la calidad de vida.

«La seguridad está estrechamente vinculada con la riqueza y el desarrollo», dice el informe. Con esto, destaca que, aun con los sistemas más modernos y la mejor infraestructura, las ciudades sus habitantes se sienten más seguros y menos homicidios registran las estadísticas son aquellas que además ofrecen salud, mejoras en la infraestructura, buenos sistemas de transporte y una serie de factores multicausales que contribuyen a reducir el delito. También señala que es complejo determinar cuál, entre varios factores de mejora, determina la seguridad. Por ejemplo, varias ciudades que se candidatearon o se prepararon como sede de Juegos Olímpicos incrementaron sus índices de seguridad: la mejora en las rutas, los subtes, la

iluminación, el planeamiento urbano, también conforman un ambiente más protegido, más allá de la instalación de cámaras, patrulleros inteligentes o policías con ojos electrónicos en sus uniformes.

Respecto de la relación entre seguridad y bienestar en las ciudades, el informe destaca un factor siempre repetido pero también ignorado: las ciudades más fragmentadas socialmente, con barrios cerrados y muros internos, son más inseguras. No importa si invierten grandes presupuestos en seguridad: si las comunidades se encierran para evitar el crimen y la violencia, generan más inseguridad. Johannesburgo, la ciudad más grande, rica y poblada de Sudáfrica, es el ejemplo. Ubicada en uno de los peores puestos de seguridad personal, con altas tasas de crímenes violentos y pandillas urbanas, su respuesta a estos peligros es el crecimiento de las comunidades cerradas: tiene 300 barrios privados. Un estudio realizado en 2013 en Sudáfrica reveló que el riesgo de robos aumentó a medida que estas comunidades crecieron. Santiago, en el peor lugar del *ranking* de seguridad personal, también incrementó el número de comunidades privadas.

Además de admitir que la seguridad sigue siendo un resultado de múltiples causas, el *ranking* de las «Ciudades seguras» demuestra que las primeras en esa categoría no son las más vigiladas. En el *top ten* se encuentra Tokio (Japón), Singapur (Singapur), Osaka (Japón), Estocolmo (Suecia), Ámsterdam (Holanda), Sydney (Australia), Zurich (Suiza), Toronto (Canadá), Melbourne (Australia) y Nueva York (Estados Unidos). Aunque todas tienen sistemas de vigilancia, ninguna de ellas está en el *ranking* de las ciudades con más cámaras del mundo. Nueva York, que tiene diez veces menos cámaras que Chicago, también tiene menos homicidios. Tokio, con 10 mil cámaras para sus 13 millones de habitantes, lidera el *ranking* de seguridad. Toronto, que se niega a seguir el camino de la vigilancia masiva (mientras debate el dilema entre seguridad y privacidad) es además una de las mejores ciudades para vivir en el mundo en otros aspectos, como la salud y la calidad de vida. En cambio, entre las ciudades más inseguras se encuentran algunas de las más vigiladas: Beijing, México DF, San Pablo.

Las cámaras en las calles, escuelas, negocios y hospitales otras veces funcionan como placebo («si está la cámara es más seguro»). Pero, así como su instalación se produce rápido y sin discusión, luego no se realizan chequeos de seguridad periódicos para asegurarse de que las imágenes no puedan robarse, alterarse, borrarse o simplemente para que nadie externo a las autoridades tenga acceso a ellas. En este aspecto, una de las razones que hacen a Tokio la ciudad más segura es que sus sistemas de monitoreo son poco vulnerables. En cambio, Moscú, en el piso de la lista, sufre vulneraciones constantes y robos informáticos frecuentes de cibercriminales. En el caso de la Argentina, los expertos en seguridad informática aseguran que pocos sistemas de

videovigilancia estatales realizan controles periódicos de seguridad y que casi el 100 % de los modelos de cámaras utilizados presentan vulnerabilidades.

Sobre la relación entre estadísticas, máquinas y declaraciones políticas, las contradicciones son infinitas. En julio de 2012, el entonces recién asumido secretario de Seguridad de la Nación, Sergio Berni, declaró[165]: «Buenos Aires es una de las ciudades más seguras de Sudamérica». Según los informes internacionales, en aquel caso de la Cepal (Comisión Económica para América Latina y el Caribe, dependiente de la ONU), su afirmación era cierta. «En la Capital, en robo seguido de muerte, tenemos una tasa de cinco por cien mil; cada cien mil habitantes, cinco homicidios. Esto la coloca dentro de las ciudades más seguras de América Latina». Sin embargo, tras esta declaración, y los años siguientes, su ministerio promovió, mediante el Plan Nacional de Protección Ciudadana, «la incorporación de recursos tecnológicos y logísticos» para «la lucha contra el delito». En el marco de ese plan están los presupuestos para la compra de sistemas de videovigilancia, tanto para la ciudad de Buenos Aires (donde la Policía Federal suma ese equipamiento al de la Policía Metropolitana local) como para los 135 distritos de la provincia de Buenos Aires, 125 de los cuales ya recibieron recursos para instalar sus centros de monitoreo.

En la provincia de Buenos Aires, donde se registran 82 delitos por hora[166] y 3 homicidios dolosos por día, el consenso sobre el estado de inseguridad es unánime y ni siquiera el partido gobernante se atreve a cuestionar que es un problema a resolver. En 2009, como una de las soluciones, se estableció el Programa Integral de Protección Ciudadana (PIPC), por el que el Gobierno nacional y el provincial se comprometían a la transferencia de recursos para la compra de tecnología de los municipios. Para los partidos significaban montos importantes de presupuesto para adquirir cámaras de vigilancia, sistemas de alarmas y reconocimiento de patentes en los ingresos a los partidos, la construcción de centrales de monitoreo y vigilancia satelital para los patrulleros, entre otras herramientas. También, dispuso en letra impresa, que «las imágenes captadas por las cámaras» fueran guardadas por los municipios «por un periodo determinado de tiempo en una sala de servidores especialmente acondicionada» para servir, «de ser solicitadas por la justicia, como medio de prueba». Aunque el programa se implementó y sigue en marcha desde hace seis años, las estadísticas no reflejaron mejoras a nivel provincial. Entre 2012 y 2013 (el último año con cifras oficiales), los homicidios dolosos crecieron un 8 % y los robos a mano armada un 21 %. Los delitos de impacto social (robo, asaltos con armas o robos agravados, entraderas, salideras, golpizas y ataques de motochorros) subieron un 15 %. Los robos de autos, uno de los delitos que las cámaras deberían prever con facilidad, aumentaron un 14 %.

Las estadísticas locales no reflejan mejoras. Los informes internacionales demuestran que las ciudades más vigiladas no son las más seguras. Los especialistas siguen destacando que la inseguridad está directamente relacionada con la desigualdad social y que sus causas múltiples no pueden resolverse con soluciones

únicas. Sin embargo, la tecnología de la videovigilancia sigue promocionándose como una solución de seguridad y los gobiernos destinando una enorme cantidad de recursos a ella.

Esta irracionalidad tiene varias explicaciones posibles. Entre ellas, existen tres muy importantes, que están relacionadas. La primera es el aura mágica que le concedemos a la tecnología para resolver problemas. Como dice el sociólogo y ensayista Christian Ferrer: «a los políticos y tecnócratas no se les ocurre otra solución que no sea técnica». Según él, el mundo vive bajo una matriz técnica, que es un poder en sí mismo, por el cual le damos a las máquinas una voluntad suprema. Podemos pensar (con mucho esfuerzo) que las tecnologías no son neutras y que arrastran daños «colaterales», pero siempre las terminamos adoptando sin prestar demasiada atención a su relación costo-beneficio.

La segunda está vinculada con la búsqueda de resultados rápidos a problemas complejos: queremos pagar por soluciones empaquetadas, comprar fórmulas de seguridad. Las empresas de tecnología son especialistas en eso, desde que nos ofrecen teléfonos que nos hacen más felices hasta sistemas de monitoreo que nos reconfortan de seguridad. Compramos tecnología como compramos caramelos: si nos gusta el paquete y creemos en su publicidad que dice que comiendo esa pastilla tendremos mejor aliento para besar a la chica, la queremos.

La tercera explicación tiene que ver con el propio sistema capitalista: las empresas que nos venden las tecnologías de vigilancia masiva son parte del problema y de la solución de la inseguridad. Siempre ofrecen un avance más para nuestras vidas alarmadas por el delito, y al mismo tiempo conocen qué despachos de funcionarios, legisladores, intendentes o presidentes visitar para venderles sus inventos fabulosos. Como en el cuento del escritor sueco Hans Christian Andersen «El traje nuevo del emperador», los soberanos creen que vestirse con más brillo (acrecentar la tecnología de sus reinos) les dará más poder, los hará más atractivos ante sus súbditos. Pero tal vez solo estén comprando lo mismo de siempre, para permanecer, como antes, desnudos.

En la última versión cinematográfica de *Robocop*[167], en una Detroit de un futuro 2028, la sociedad está dividida frente a una pregunta: «¿Podemos dejar la seguridad en manos de aparatos sin corazón ni sentimientos, dirigidos desde una pantalla o un programa de computación?». Omnicorp, la poderosa empresa de ficción que vende los robots-armas está decidida a que la respuesta sea sí. El negocio de la seguridad es demasiado grande como para dejarlo en manos de otros. Entonces se propone convencer a la opinión púbica de que la tecnología puede tener un «costado humano». Para eso, hay que encontrar una historia y un personaje. Así nace Robocop, un robot semihumano, capaz de procesar los registros criminales, huellas digitales e información de toda una ciudad en pos de luchar contra el crimen. Sin embargo, en

sus primeras misiones se descubre que su parte humana todavía tiene conciencia y miedos. Omnicorp entonces lo convierte en una máquina y le crea a él y a la sociedad la ilusión del libre albedrío: los hace pensar que todavía deciden sobre la vida y la muerte, cuando en realidad solo lo hacen las máquinas. Pero esas máquinas no actúan solas. Están controladas por un pequeño grupo de hombres: aquellos que las programan.

Robocop muestra, en un escenario distópico, algo que vivimos todos los días. ¿Quién decide sobre la vida y la muerte? ¿Una sociedad, a través de un debate público sobre qué métodos usar y cuánto gastar? ¿O esas decisiones sobre temas tan delicados se toman a puertas cerradas, en las oficinas de quienes compran la tecnología: funcionarios, representantes de las empresas de tecnología, legisladores que aprueban presupuestos?

«La vigilancia masiva es una política con un modelo de negocios[168]», dice el periodista de tecnología canadiense Cory Doctorow. «Espiar a todos tal vez no atrapa terroristas, pero sí hace a los contratistas militares y a las empresas de telecomunicaciones ganar un montón de dinero». Doctorow señala que vivimos la paradoja de un mundo que se supone cada vez más eficiente, pero donde se toman decisiones basadas en evidencias futuras: usemos estas tecnologías porque nos permitirán resolver un problema. ¿Quién lo dice? Las mismas empresas que venden las soluciones, con sus modelos de negocios adaptados a «lo que necesita la política». En ese camino, «se crea una gran riqueza para un pequeño número de jugadores, que tienen el dinero suficiente para hacer *lobby* para que se continúen tomando esas decisiones de política».

En el caso de la tecnología aplicada a la vigilancia y la seguridad, el *marketing* es muy agresivo, porque se combina con un avance real de las máquinas. Pero, señala Doctorow, no hay que olvidar que, aun cuando las tecnologías sean nuevas, la forma en que se toman las decisiones sobre su compra e implementación por parte de los Estados es la misma que para otros negocios privados que se deciden en almuerzos lujosos, viajes financiados por las empresas para que los funcionarios visiten «casos de éxito», licitaciones que se ganan por contactos políticos.

En la Argentina, tres empresas se reparten la instalación y el mantenimiento de los sistemas de videovigilancia en los municipios[169]. No solo venden las cámaras, sino también equipos de seguimiento satelital, dan soporte técnico y se encargan de las redes de fibra óptica necesarias para transmitir las imágenes. Las relaciones que establecen estas compañías con los municipios son vitales, ya que son ellos los que manejan los presupuestos para tecnologías de seguridad que reciben desde los gobiernos provinciales o nacionales, pero también las que otras veces deciden destinar partidas económicas propias «a pedido de los vecinos». El poder de estas

empresas es el *lobby* y como en otros negocios de la tecnología se trata de monopolios que se reparten un territorio para vender sus productos[170].

La primera es Telefónica Ingeniería de Seguridad (TIS), de la multinacional Telefónica, cuya ventaja comparativa es ser dueña de redes de telecomunicaciones y fibra óptica. Con esto, puede ofrecer «paquetes» de videovigilancia y contar con su propia infraestructura para transmitir las imágenes y los datos. En su página oferta los combos necesarios para la seguridad, entre ellos centros de monitoreo «llave en mano»: instala todo, lo deja funcionando y lo mantiene. No solo los ofrece a municipios[171], sino a todo tipo de lugares que requieran de sistemas de CCTV: hospitales, aeropuertos, cárceles, fábricas, galerías de arte. Telefónica tiene excelentes relaciones con el kirchnerismo, pero también las tuvo con todos los gobiernos anteriores, desde que se hizo cargo del servicio telefónico luego de la privatización de Entel en 1990. Además, tiene vínculos con empresarios de medios de comunicación como Sergio Szpolski, señalado como propietario del 6 % de las acciones de la compañía, y de colaborar mediante su cercanía con el gobierno kirchnerista con la llegada de la empresa a la adjudicación de licitaciones.

La segunda empresa es Ubik2, especializada en sistemas satelitales, y fundada en 2008, poco después de la asunción de Daniel Scioli como gobernador de la provincia de Buenos Aires y de que este comenzara a invertir grandes sumas del presupuesto de seguridad en cámaras. Uno de sus gerentes, Rodrigo Campbell, licenciado en Transporte y Logística por la Universidad de la Marina Mercante, fue vicepresidente de la Cámara Argentina de Empresas de Seguridad e Investigación y tiene cercanía con el kichnerismo, varios de cuyos municipios se armaron de sistemas de videovigilancia a través de Ubik2. La empresa opera desde Ezeiza —tierra del actual ministro de Seguridad bonaerense, Alejandro Granados, uno de los primeros entusiastas de las cámaras— y desde allí provee a municipios como Ituzaingó, Florencio Varela y el Partido de la Costa. El discurso de Campbell en los medios está estudiado con precisión: se refiere a los sistemas de vigilancia con una jerga técnica (utiliza el neologismo «video observación urbana»), siempre asociada a «soluciones», que evita nombrar a las personas.

La tercera empresa, Global View, es la más poderosa. Su nombre es sinónimo de videovigilancia en la Argentina, de ganar licitaciones para sistemas de seguridad y de los vínculos más estrechos con el poder nacional e internacional. Su fundador es Mario Montoto[172], un exintegrante de la agrupación Montoneros que fue mano derecha de Mario Firmenich, uno de los líderes de la organización durante los 70. Nacido en La Plata en 1956, militante peronista desde la escuela secundaria, Montoto se dedica hace más de dos décadas al negocio de la videovigilancia, la industria bélica y la consultoría sobre narcotráfico y amenazas transnacionales. Fundó Global View en 2008, pero había instalado la primera cámara de seguridad a principios de los años 80, en México, «en frente de una casa donde vivía con otra gente», sus compañeros exiliados de militancia política. En los 90, luego de los indultos del

gobierno de Carlos Menem a militares y a su exjefe Firmenich, Montoto dejó la militancia política y se dedicó a la actividad privada. Desde allí a la actualidad hizo sus negocios en y con todos los gobiernos: comercializó vinos, fue empresario metalúrgico, de transporte y de ferrocarriles.

En 2003 fundó Codesur (Corporación para la Defensa del Sur), compañía que todavía preside y que se dedica a la venta de productos y servicios para la industria bélica. «Porque queremos la paz, trabajamos para la defensa y la seguridad interior», dice el eslogan de la página web de su empresa, que se encarga desde la venta de equipamiento para la Fuerza Aérea, la Marina y el Ejército, pasando por la capacitación de pilotos y fuerzas de seguridad, hasta de proveer «equipamiento para la guerra electrónica» y «custodias vip». Todo «listo para usar», garantiza Montoto. Sus clientes son las Fuerzas Armadas, las policías y todos los niveles de gobierno, que lo contratan para mantener submarinos, reparar helicópteros del Ejército o mantener aviones presidenciales. El plantel directivo de su empresa lo garantiza: entre sus integrantes hay un general de división, un brigadier y un vicealmirante, todos retirados. Quienes lo persiguieron a Montoto en los 70 (y asesinaron a su primera esposa en un operativo del Plan Cóndor en Perú) son hoy sus socios de negocio, y sus clientes.

Además de centralizar sus actividades en Codesur, Montoto tiene un gran manejo de dos áreas fundamentales del poder: los medios de comunicación y los funcionarios de todos los gobiernos. Desde su oficina de Puerto Madero, con cinco relojes que marcan las horas de Beijing, Washington, Buenos Aires, Tel Aviv y Madrid, Montoto admite que una de sus virtudes es llevarse bien con todos: «No me peleé con Menem, con De la Rúa ni con Duhalde. No me voy a pelear con los Kirchner», admite[173]. También acepta que se lleva bien con el secretario de Seguridad, Sergio Berni, con el gobernador de la provincia de Buenos Aires, Daniel Scioli, y con el ministro de Seguridad de la ciudad de Buenos Aires, Guillermo Montenegro. A todos ellos, junto a dirigentes de La Cámpora, los reunió en noviembre de 2014 en un congreso sobre «seguridad hemisférica», una de las actividades que desarrolla bajo el paraguas de la Fundación Tadea, que también edita libros y realiza capacitaciones en temas de defensa y seguridad. En el ámbito de los medios, Montoto también es el responsable de la revista *DEF* (dedicada a temas de defensa) y del programa de televisión *Def TV*, al frente de los cuales está el coronel retirado Gustavo Gorriz. Global View, su empresa dedicada a la videovigilancia, también tuvo lazos con el mundo televisivo, con vínculos comerciales con el empresario de medios Daniel Hadad cuando este era propietario de la señal de cable C5N (luego vendida al grupo de medios Indalo, vinculado con el kirchnerismo).

En Global View Montoto centralizó sus negocios del rubro videovigilancia desde 2008. La empresa se adjudicó las licitaciones de sistemas de CCTV más importantes del país para grandes localidades de la provincia de Buenos Aires, como Lomas de Zamora, Tigre, Campana, Escobar, Lanús y Mar del Plata. También tiene contratos

con el Ministerio de Seguridad de la Nación (por ejemplo, para las cámaras de la Policía Federal en la ciudad de Buenos Aires) y con el Gobierno de la ciudad de Buenos Aires, para los servicios de cámaras y mantenimiento del sistema de la Policía Metropolitana, y ganó las licitaciones en grandes centros urbanos del país, como Rosario.

En febrero de 2012, Montoto vendió Global View a la multinacional japonesa NEC, líder mundial en el rubro. La venta (cuyo mayor capital es su gran influencia en las licitaciones y las relaciones ya establecidas con quienes toman las decisiones de la compra de materiales de videovigilancia en los municipios[174]) fue valuada en 30 millones de dólares y el empresario argentino se quedó con el 15 % de las acciones[175]. Al frente de la empresa, en la presidencia de NEC Argentina, está Carlos Martinangeli, un hombre cercano al ministro kirchnerista Aníbal Fernández, no solo políticamente sino porque ambos ocupan la comisión directiva del club de fútbol Quilmes. Pero, al contrario del club de su pasión, con destinos deportivos imprevisibles, el negocio de las cámaras le ofrece seguridad: «Latinoamérica es un mercado potencial muy grande para la videovigilancia, porque no está explotado. Queremos que Global View sea la empresa del rubro más grande del mundo», declaró Martinangeli. Mientras, NEC Argentina ya controla el mercado de los sistemas de identificación por huellas dactilares en dependencias del Gobierno nacional como el Ministerio del Interior. La influencia de Montoto es tan importante que él mismo acompañó al gobernador Daniel Scioli a Jerusalén, Israel[176], para comprar los insumos del centro de monitoreo que se instaló en La Plata, la capital de la provincia.

Los lazos entre los empresarios de la seguridad dedicados a la videovigilancia, las altas esferas de la decisión política y los medios de comunicación son evidentes. Los dueños de las compañías no figuran en las páginas de las empresas pero no se esconden de las fotos en encuentros políticos o mediáticos. Los vínculos también resultan, periódicamente, en acusaciones de corrupción en las licitaciones, o en manejos poco claros de los presupuestos, que son siempre adjudicados a las mismas compañías, o que muestran irregularidades. En febrero de 2011, la ciudad de Bahía Blanca se hizo eco de un escándalo cuando Mario Montoto declaró en el canal de cable C5N haber resultado ganador de una licitación de 50 cámaras antes de que la misma hubiera terminado[177]. En otras ciudades se repitieron las denuncias de corrupción. Sin embargo, el avance de las cámaras y los centros de monitoreo siguió adelante.

En las decisiones sobre la videovigilancia y otras inversiones públicas de tecnología el mercado todavía se impone por sobre la deliberación pública. En la historia, esto no es algo nuevo: las ciudades, a medida que crecieron, fueron grandes consumidoras de nuevas tecnologías. La relación fue siempre simbiótica: desde el telégrafo conectando las urbes en expansión a fines del siglo XIX, los teléfonos haciendo más eficiente la gestión de las oficinas públicas hacia 1910, hasta las ciudades de hoy que reemplazan las filas para sacar turnos de trámites por

aplicaciones móviles, todo lo que rodea nuestras ciudades es tecnología. O conviene que así sea.

En los últimos años se habla sin pausa de las «ciudades inteligentes» o las «*smart cities*» como una novedad y un hecho de progreso tan positivo como incuestionable. Sin embargo, las *smart cities* son muchas cosas a la vez, pero sobre todo, un nuevo argumento para que las grandes empresas de tecnología vendan sus productos. IBM, Siemens, General Electric y Cisco, entre otras, saben de qué se trata, porque ya vendieron, cien años atrás, telégrafos, teléfonos, luz eléctrica y ahora caños de internet. Son ellas mismas las que hoy venden *software*, celulares conectados a 4G o *wifi*, aplicaciones para gobiernos, sistemas de vigilancia y biometría. El investigador de la Universidad de Nueva York Anthony Townsend señala que, paradójicamente, incluso estas mismas empresas que contribuyeron a producir las consecuencias más graves del avance de las ciudades en el siglo XX (congestión, calentamiento global, déficit de salud) son las mismas que proponen las soluciones para remediar estos problemas en el siglo XXI. ¿Cómo? A través de sensores, programas, redes y controles automatizados de todos nuestros movimientos y datos, para medirlos, hacer cálculos, determinar qué necesitamos y hacer más «eficientes» las respuestas de los gobiernos ante esos problemas. «Donde había gasto, habrá eficiencia. Donde había riesgo, habrá predicciones y advertencias antes de tiempo. Donde había crimen e inseguridad, habrá ojos que todo lo ven. Donde antes había filas, tendremos servicios de gobierno abiertos**[178]**».

Es cierto: para algunos problemas, la tecnología es una solución. Nadie se negaría a perder menos tiempo en un trámite que puede hacerse completamente *online*, a ignorar la información de mapas de tránsito «inteligentes» en horas pico, a proveer de dispositivos de alerta a mujeres en riesgo de violencia. Sin embargo, para muchas de estas y otras soluciones, siempre hay un precio que pagar: esos datos los maneja alguien. Puede ser un gobierno, con reglas claras (o no tan claras) de manipulación de información y cuidado de la privacidad. Pero también lo administran las compañías. El escenario es complejo. Ni las empresas actúan todas en perjuicio de la gente, ni los gobiernos solo hacen negocios espurios, ni todo tiene consecuencias negativas. Sin embargo, los grandes presupuestos se siguen manejando a través de empresarios que hacen *lobby* y políticos que necesitan «mostrar gestión». Si eso implica llenar las calles de cámaras es bienvenido. Si además esas imágenes luego llegan a los medios, y muestran más acción, es aún mejor.

En una noche desesperada de su vida, Lou Bloom descubre que en su ciudad, Los Ángeles, existen camarógrafos aficionados que filman accidentes de autos, persecuciones, robos y tiroteos, y los venden a los canales de cable locales. Acorralado por ganar dinero, consigue una cámara, intercepta la frecuencia de la policía y ofrece las imágenes a la productora de un noticiero local desesperada por

mejorar su *rating*. Semana a semana, Lou advierte que cuanto más violentos son los materiales sus pagos aumentan. También descubre que si las noticias no existen puede inventarlas, o al menos modificar un poco la realidad para que sucedan. En definitiva, lo que necesita cada noche el noticiero son imágenes impactantes. Si son ciertas o no, es secundario.

La historia pertenece a *Nightcrawler*, una película de 2014 que ni siquiera se estrenó en Argentina, pero plantea una situación muy actual de los medios y su necesidad permanente de «conseguir cámaras». Así las piden los productores a los encargados de prensa de las ciudades que todo lo filman: «¿Tenés una cámara?». Los encargados de prensa de los municipios —llamados en la jerga «prenseros»—, las envían. Para ellos es una forma de «mostrar gestión»: de que su localidad no solo está persiguiendo delincuentes, sino que, además, tiene la evidencia de que lo hace. Para los noticieros argentinos las imágenes son un flujo constante y gratuito de minutos de programación para sus horas al aire, en especial, de los noticieros principales de las siete de la tarde, que tienen predilección por abrir sus emisiones con noticias de seguridad. Para los canales de cable el material de las cámaras permite no solo repetir los hechos delictivos varias veces al día, sino que algunos también cuentan con programas enteros realizados íntegramente con esas imágenes.

La relación simbiótica de las cámaras de seguridad con los medios de comunicación es tan grande que algunos de los materiales que ellas obtienen llegan incluso a usarse o cederse para publicidades. Eso ocurrió en el caso del «Héroe de Tigre», un hombre que corrió sobre las vías del tren segundos antes de que la formación pasara para mover un camión que había quedado parado sobre ellas y que si no hubiera sido aplastado. El vehículo y el hombre resultaron ilesos y el tren pasó sin matar a nadie. Meses después, la imagen se convirtió en parte de «Camaritas», una publicidad creada para Coca-Cola por la filial Argentina de Young & Rubicam y fue el primer aviso nacional en llegar a la tanda comercial del Superbowl de Estados Unidos, donde lo vieron 100 millones de personas en simultáneo[179]. Para crearlo, la agencia instaló cámaras «ocultas» que captaran imágenes que demostraran que la gente realiza acciones de bondad y valentía aun cuando nadie la mira. En ese video el «Héroe de Tigre» aparece como uno de los valientes y el municipio de Tigre —que cedió esa imagen luego de consultar con el hombre— figura con su marca en el comercial que recorrió el mundo. Cuando se estrenó en las redes sociales los comentarios fueron en su mayoría positivos. Su recorrido internacional también fue exitoso: «Camaritas» fue elegido como el mejor aviso por los televidentes del Superbowl 2012.

Con su presencia en las noticias y hasta en la publicidad, las imágenes de las cámaras de seguridad van legitimando su aparición en los medios. Son recibidas como una forma de «combatir la inseguridad» en forma de ojos que eliminan a los delincuentes con su sola presencia. Pero también como una forma de *vigilantenimiento* (una mezcla de vigilancia con entretenimiento), que es utilizada por

la publicidad con un *marketing* positivo de las emociones, como sucede con el aviso de Coca-Cola.

Aceptamos las cámaras, por una razón u otra, y de esa forma les vamos permitiendo interactuar con nuestros cuerpos, camufladas en el espacio público. También los ojos electrónicos privados, dispuestos sobre nosotros en edificios, negocios y empresas, a quienes no les cuestionamos su presencia ni que nos saquen una foto para el ingreso a una oficina**[180]** (a no ser que tengamos el tiempo y la paciencia de discutir con empleados y recepcionistas). Hay, incluso, cámaras que nos registran sin permiso y que además celebramos, como las de los camiones de Google Street View que filman nuestras ciudades (y a nosotros) para convertirse en parte de una aplicación de la empresa.

Pero mientras la vigilancia se extiende y convivimos con ella aparecen nuevas preguntas, conflictos y dilemas. Las preguntas tienen respuestas ocultas o que están siendo todavía debatidas. Entre ellas: ¿dónde están ubicadas las cámaras?, ¿pueden estar camufladas, ocultas, o tenemos derecho a conocer los lugares desde donde nos registran?, ¿cuánto tiempo se pueden guardar las imágenes y para qué fines se pueden utilizar?, ¿los medios pueden tener acceso a ellas? Los dilemas retoman el difícil equilibrio entre el derecho a la seguridad y el derecho a la privacidad. ¿Qué derechos dejamos de lado con tal de garantizar la seguridad? ¿Hay una forma buena y una forma mala de ser vigilados? ¿La privacidad —o lo que conocíamos como ella— está condenada a desaparecer? ¿Podemos reclamarla, o debemos aceptar su final?

En la ciudad de Buenos Aires, la ley 2602 de 2007 regula el funcionamiento de las cámaras en el distrito**[181]**. Es obligación de las autoridades señalizarlas, para que los vecinos sepan que están siendo vigilados. Junto con esta norma, el uso de las cámaras también debe respetar ley 1845 (de 2005), de Protección de Datos Personales, que resguarda las imágenes como un dato de carácter personal que debe ser tratado sin violentar el derecho a la privacidad. Esto significa que, aun en el espacio público, las personas tenemos un derecho y una expectativa de privacidad y anonimato, garantizado por diversas normas nacionales e internacionales de derechos humanos**[182]**.

En la ciudad de Buenos Aires, las imágenes se guardan 60 días. Se almacenan en el centro de datos de la Policía Metropolitana en Barracas, con el fin de responder a los pedidos judiciales que las requieran como prueba. En el país y en el mundo, los tiempos de guardado varían entre dos semanas y dos meses, tiempo suficiente para colaborar con la justicia. Internacionalmente, el consenso es que no es razonable retener la información por más tiempo, ya que cualquier causa legal se desarrolla en esos tiempo. Archivar más las imágenes violaría los derechos de las personas porque implicaría, por ejemplo, realizar una acumulación de datos sobre una persona.

El tiempo de guardado de las imágenes, sin embargo, no es el aspecto que genera más conflictos de derechos. Sí suele haber problemas con la identificación pública de las cámaras y con la cesión de las imágenes a los medios. En la ciudad de Buenos

Aires, la Defensoría del Pueblo, a través de su Dirección de Protección de Datos Personales, se ha encargado de tomar cartas en el asunto en algunos de estos temas. En 2013, el sociólogo Andrés Pérez Esquivel llevó a ese organismo un pedido para que el Ministerio de Justicia y Seguridad de la ciudad entregara un listado de ubicación de las cámaras. La respuesta fue que esa información era «confidencial» y a los pocos días incluso dio de baja la información de la locación de las cámaras de su página web. La Defensoría había recibido una negativa similar, que se sumaba a la respuesta del ministro de Seguridad Montenegro en una audiencia en la Legislatura, donde alegaba que revelar el lugar de las cámaras favorecía a los delincuentes a cometer delitos. Pero esto contradecía la propia letra de la ley, que establece que las cámaras son preventivas, y por lo tanto, si los vecinos conocen donde están las cámaras les permitiría saber «si están siendo víctimas de un robo, disuadir la intención del atacante indicándole que está siendo filmado o incluso acercarse a la cámara más cercana y llamar al 103 ante cualquier peligro, en caso de no contar con presencia policial». Además, aclaró el sociólogo: «El delito organizado siempre realiza un relevamiento visual previo de ubicación de cámaras en el territorio donde tiene pensado actuar», por lo que a los únicos que perjudicaba el secretismo era a los habitantes de la ciudad. Finalmente, el Ministerio hizo pública la ubicación exacta de las cámaras y las publicó en sus sitios web oficiales**[183]**.

La paradoja de las autoridades que se niegan a publicar dónde están las cámaras a los ciudadanos es que, al mismo tiempo, las entregan permanentemente a los canales de televisión. Eso sucedió en 2011, cuando, según relata Pérez Esquivel, «el ministro de Seguridad porteño creó el programa Pronto Baires, con el objetivo de *responder de manera rápida y eficiente a la demanda de información por parte de los medios de prensa*, y sancionó la resolución N.º 314/11 para crear convenios con canales de televisión». Luego el funcionario negó públicamente haber firmado ese documento, pero también ya se había conocido que para dar servicios a Pronto Baires había contratado a la consultora AR y Asociados, que tenía vinculaciones comerciales con Global View, la empresa de Mario Montoto que había instalado las cámaras de seguridad**[184]**. Además, uno de los directores de Global View había sido gerente de Canal 9 y C5N, que accedían y mostraban en sus pantallas las imágenes de las cámaras de seguridad.

El círculo es el mismo que se produce en Tigre y en otros municipios de la Argentina: los funcionarios declaran que las cámaras se instalan para prevenir el delito, pero —aunque eso pueda o no suceder— luego también las usan para sus propias campañas de *marketing* en los medios o como recursos de campañas electorales. Pérez Esquivel señala que en ese espiral radica un peligro llamado «La paradoja del in fraganti», descrito por su colega brasilero Bruno Cardoso de la Universidad de Río de Janeiro: «Cuando se promocionan los videos exitosos se reproduce la necesidad política y operativa de producir más videos, para lo cual se

necesita que haya más delitos que ocurran frente a las cámaras, al mismo tiempo que se los intenta disminuir».

También se generan conflictos por la privacidad de las imágenes y la intromisión en la intimidad de las personas. La Defensoría del Pueblo de la Ciudad de Buenos Aires actuó en varios, resolviendo que «la colocación de las cámaras debe realizarse en lugares donde la privacidad de las personas no se vea vulnerada». Concluyó entonces que una empresa debía modificar la colocación de cámaras en el ámbito de trabajo para resguardar la imagen de sus trabajadores, e intervino en un caso para que la Policía Metropolitana cambiara de lugar una cámara que se había instalado apuntando hacia el interior del baño de un vecino. También actuó en un pedido para que Google informara dónde se guardaban las imágenes de las cámaras que filmaron durante varios meses la ciudad de Buenos Aires para compilarlas cuadra por cuadra en la aplicación Street View. La empresa respondió que el vehículo con la cámara estaba aprobado para realizar esa acción, pero no aclaró dónde guardaba las imágenes ni por cuánto tiempo, aunque luego se supo que estaban almacenadas en Bélgica.

El de Google Street View fue uno de los pocos casos en donde hubo, en la Argentina, un mínimo debate acerca de la privacidad en el ámbito público, aunque en ese caso no relacionado con la seguridad. En octubre de 2013 se lanzó localmente esta aplicación[185] basada en Google Maps, que permite recorrer distintos lugares del mundo con imágenes detalladas, en forma de película, y para la cual se filmaron las calles de Buenos Aires, Córdoba, Rosario y Mar del Plata (y su gente) con un camión pintado con los colores de la compañía y una cámara panorámica sobre el techo. La aplicación es —efectivamente— divertida, por momentos adictiva, especial para perder el tiempo en internet, el vicio universal de la época. Es lógico emocionarse encontrando la escuela de nuestra infancia, viajar por paisajes a los que nunca podríamos ir o reírse de *graffitti* ingeniosos o pasacalles de amores desencontrados. Como muestra de su éxito, la página de Facebook «Street View Argento» se colmó de imágenes capturadas por personas que enviaban sus descubrimientos de Street View con imágenes que iban desde simpáticos enanos de jardín y nombres de negocios graciosos hasta otras no tan alegres como redadas de la policía atrapando delincuentes o mujeres en situación de explotación sexual en una esquina de Buenos Aires. Puesta la herramienta en nuestras manos (la posibilidad de mirar y copiar las imágenes tomadas con las cámaras de otros), la respuesta es celebrar que nos miren, al punto de compartirlo con otros sin pensar que esa persona de quienes nos reímos o distribuimos su intimidad mañana podemos ser nosotros.

La pregunta, ya sin pensar en la vigilancia del Estado, de los privados, o entre nosotros mismos al tomarle un video o una foto a cualquiera que está en la calle y subirla a Instagram o a nuestras redes sociales sin consultarle si está de acuerdo, es: ¿hay una vigilancia mala y una vigilancia buena? Si la filmación de nuestras vidas avanza inexorablemente, ¿cómo pensar el límite entre lo público y lo privado en el futuro?

Si otros interrogantes pueden ser respondidos con estadísticas de delitos, con índices de inseguridad o con leyes que nos protegen, existe un espacio gris que nos corresponde pensar a cada uno.

En 1998, a los 18 años, me mudé de La Plata a Buenos Aires. Lo que más disfruté en los primeros años fue la sensación del anonimato. Me deleitaba ese parecido a estar de viaje que viene con liberarse de miradas ajenas. Dieciséis años después, consciente de las cámaras que me miran cuando salgo a la calle, me pregunto dónde quedó ese placer de no ser nadie. Es una pregunta que nos tendremos que responder, tal vez, en la intimidad. Sin embargo, esa es una parte de la respuesta. Hay otra parte que tiene que ver con las consecuencias públicas del fin de la privacidad, y es: qué lugar queda para lo no previsto, para la libertad de acción, incluso para los actos de rebeldía (los privados y los públicos).

Oscurecía cuando, en el verano de 2015, salí del Centro de Operaciones de Tigre repleto de pantallas con escenas de cámaras de seguridad. En el camino, era difícil no estar pendiente de los cientos de ojos que ahora sabía con precisión que me estaban registrando hasta llegar a la estación del tren que me llevaría de vuelta a la Retiro, en la ciudad de Buenos Aires, donde otras cientos de cámaras me iban a custodiar hasta llegar a mi casa. Ya no había ingenuidad: las veía a mi paso en las esquinas, sobre los postes de la ruta, doblando la avenida circunvalación, en el puente donde miles de turistas cruzaban hacia las islas del Delta el fin de semana.

Cuando llegué a la estación ya era de noche. Dos policías custodiaban, de cada lado de las boleterías, a la gente que pasaba su tarjeta Sube por el molinete para ingresar al andén. Después de franquear mi vuelta hacia el lugar de espera de los trenes, con poca gente, en un día de semana, miré hacia arriba. Tres cámaras nos miraban: a mí, a los policías, a todos los que compartíamos la llegada del primer convoy para partir. Volví a mirar y me encontré pensando si esos ojos en forma de esfera no me estaban dando, en ese momento y sin pensar en mis prejuicios, algo de seguridad. Intenté evitarlo: no quiero que a mí también me pase, no quiero pensar que la tecnología me protege a cambio de mirar cada cosa que hago mientras espero el tren, miro los chistes, los empujones o los besos de esos chicos que están esperando aquí conmigo. Por un instante, ese pensamiento me ganó.

Sin embargo, ya en el tren, pensé en las otras veces que lo había tomado, años atrás, en esa misma estación, y no me había pasado nada. Recordé, también, en las veces que, en ese mismo tren, me besé con un novio volviendo de un fin de semana en el Delta y cómo me sentiría de saberlo hoy. Repasé a las otras personas cuyas imágenes vigiladas llegan a los medios: jóvenes, pobres, con el prejuicio de que juventud y marginalidad significan mantenerlos bajo la raya de una cámara para que no cometan otros actos contra la sociedad.

Finalmente, pensé en mi infancia, todavía durante la dictadura, en La Plata. Mis padres y otros padres, todavía vigilados al salir de sus casas por las fuerzas de seguridad. Los viajes a la plaza, en el cochecito de bebé, con esos hombres (todavía no máquinas de vigilancia) que nos seguían para asegurarse de que efectivamente estuviéramos paseando al sol y no encontrándonos para conspirar contra el régimen. Me acordé, entonces, de mi charla con Claudio Ruiz, el abogado y activista chileno de Derechos Digitales, nacido, como yo, a fines de los 70:

—Hace unos meses tuve que hablar en un encuentro sobre vigilancia en el Parlamento inglés —me dijo—. Y allí, en un país hipervigilado, dije que me resultaba extraño que en América Latina no nos preocupe más la vigilancia. Porque nosotros nacimos en una sociedad vigilada. No tecnológica, pero yo recuerdo patente que en mi infancia, con mi padre dirigente sindical y militante, llamaban todos los días al teléfono de mi casa. La orden era que yo, un niño, tenía que atender y negar que él estuviera allí.

—Es decir, conocimos de niños la idea de vigilancia, aunque no supiéramos bien de qué se trataba.

—Claro, a los 7 años, es una instrucción: «Atiende el teléfono y no permitas que sepan dónde estamos». Pero ahora, treinta años después, ¿qué cambió para que lo aceptemos sin cuestionar de dónde viene la orden?

IX

Dar aceptar: Google, Facebook y WhatsApp se apropian de nuestros datos

> «Durante décadas, las computadoras nos ayudaron a recordar, pero ahora es tiempo de que nos ayuden a ignorar».
>
> CORY DOCTOROW.

«El monitoreo total es inevitable.

Esconderlo, mentir sobre él, no lo es».

KEVIN KELLY.

Cuando cumplí cinco años en mi trabajo mi jefe me regaló un reloj inteligente. El pequeño aparato, de tres centímetros por cuatro, 150 gramos de peso con caja incluida, estaba fabricado para adaptarse a mi vida. Con una batería diseñada para durar siete días, capacidad para sumergirse 50 metros en agua, recibir mensajes, llamados y escuchar mi música preferida, era el compañero perfecto para el exilio en una isla desierta.

Mi jefe, un ingeniero genuinamente apasionado por la tecnología, pensó que el reloj era el mejor regalo para experimentar lo que el *marketing* llama la «vida *smart*»: objetos que se adaptan al ambiente y a nuestras costumbres, a cambio de que les demos información para que eso suceda.

«Encuéntrate con Pebble, el reloj inteligente que se vuelve más inteligente con las nuevas aplicaciones creadas diariamente», decía la caja de diseño minimalista, blanca, el mismo color del *gadget*. Detrás de un envoltorio transparente, sus especificaciones de fábrica me aseguraban que, si lo extraía de ese cofre de cartón y decidía atarlo a mi muñeca, podía mantenerme conectada al mundo durante una semana prescindiendo de la electricidad. Me permitía, incluso, personalizar la pantalla con la cara de mi mascota.

Pero nunca me gustaron las mascotas. La idea de un animal que depende de que lo alimente a cambio de vivir encerrado en la ciudad siempre me pareció triste. El reloj era como un animal. Solo que en vez de comida y un pote de agua diario, me pedía algo —tal vez menos tangible pero más valioso— para convertirse en mi compañero de vida más eficiente: todos los datos de mis llamadas, contactos, *mails*, preferencias musicales, imágenes, mis interacciones en las redes sociales. Y me

prometía que, en el futuro, a medida que fuera sumando nuevas aplicaciones para hacerme la vida más eficiente, también me pediría otros detalles personales: mi pulso, el recorrido de mis caminatas diarias a través del GPS, las calorías que consumía diariamente y otros datos de mi cuerpo.

Extraer el reloj de la caja, pensé, implicaba un costo muy alto. No solo suponía sacrificar mi naturaleza ajena a la dependencia, sino que significaba darle a ese pequeño aparato toda mi información personal (para que siempre pudiera ubicarme, comunicarme, ofrecerme el producto o servicio exacto que necesitara). Era entregarle a ese fragmento de plástico, zinc y titanio cada huella de mi vida digital. Pero el trato no era solo con un objeto. Al firmar el contrato, a través de sus términos y condiciones, también lo hacía con la empresa que lo había fabricado, con los desarrolladores del programa que ahora gestionaría mis datos, y con quienes se proponían administrar esa información que yo dejaría en las aplicaciones y servicios. Les daba, para que dispusieran de ella, mi presencia permanente, mi comunicación sin cortes, para que siempre pudieran encontrarme y saber de mí. Con eso, también les decía con quién y dónde estaba, con quién hablaba, a quién le decía «te amo».

En 1962, en su «Preámbulo a las instrucciones para dar cuerda al reloj[186]», Julio Cortázar escribía que cuando te regalan un reloj no te ofrecen «solamente ese menudo picapedrero que te atarás a la muñeca y pasearás contigo». Te regalan, decía, «un nuevo pedazo frágil y precario de ti mismo, algo que es tuyo pero no es tu cuerpo, que hay que atar a tu cuerpo con su correa como un bracito desesperado colgándose de tu muñeca. Te regalan la necesidad de darle cuerda todos los días, la obligación de darle cuerda para que siga siendo un reloj; te regalan la obsesión de atender a la hora exacta en las vitrinas de las joyerías, en el anuncio por la radio, en el servicio telefónico. Te regalan el miedo de perderlo, de que te lo roben, de que se te caiga al suelo y se rompa. Te regalan su marca, y la seguridad de que es una marca mejor que las otras, te regalan la tendencia de comparar tu reloj con los demás relojes. No te regalan un reloj, tú eres el regalado, a ti te ofrecen para el cumpleaños del reloj».

Hoy, a más de cincuenta años de la publicación de ese cuento, el poder de los objetos y la tecnología sobre nuestras vidas sigue siendo el mismo. O peor. Ya no le damos cuerda a un reloj, pero mantenemos cargados y conectados toda clase de aparatos para confiarles a ellos y a los programas que los gobiernan nuestro tiempo, nuestras ansiedades, gustos, relaciones, consumos, búsquedas, problemas, alegrías y miedos. Todo en forma de datos. Datos de todo tipo, que pueden distinguirnos —o como se dice «construir nuestro perfil»— si los ponemos uno al lado del otro: sexo, edad, lugares que visitamos, cosas que nos gustan, gente con la que hablamos. Todos esos datos *somos* nosotros.

El aparato al que le cedemos esa información puede tener forma de reloj inteligente o de teléfono móvil o de computadora o de *smart TV*, o de cualquier cosa que se conecte a una red para intercambiar información. Nos gusta, además, coleccionar objetos, hacerlos interactuar entre sí. Si estamos lejos de uno siempre está

el otro: dejamos el celular, pasamos a la tableta, prendemos la computadora. Al teléfono celular, incluso, le pedimos tanto que no lo concebimos lejos. Los llevamos a la cama, al baño, nos acompaña mientras trabajamos, o cuando vamos al cine, cenamos, viajamos, estamos en la playa o en el aeropuerto. Ya no podemos estar sin él. Pero tampoco podemos *ser* sin él. Porque nos resuelve muchas cosas: es un teléfono, un reproductor de música, una cámara de fotos, un entrenador personal, una secretaria de citas, un buscador de noticias y restaurantes, una forma de encontrar amor, sexo, diversión, de mantenernos cerca de quienes queremos, o de husmear en las vidas de los que odiamos, de comentar en las redes sociales y de mostrar dónde estamos o queremos estar. Y en vez de vivir pendientes de darle cuerda para que nunca deje de funcionar ahora buscamos desesperados el enchufe o la batería, el *wifi* o el 4G. Cuando la electricidad falla o cuando la conexión desaparece, nos sentimos perdidos.

Como dice el antropólogo y escritor Néstor García Canclini, así como en su momento el reloj fue imprescindible y su falta generaba algunos miedos, ahora esos temores se trasladaron al teléfono móvil: tememos perderlo, que nos lo roben, que se rompa, perder la conexión. Y nos apuramos a cambiar el modelo o la marca cuando aparece en el mercado uno nuevo. «El reloj y el móvil requieren un gasto inicial, pero los móviles se diferencian porque solo existen si seguimos invirtiendo», dice**[187]**. También señala la doble vida de una era donde nos suponemos libres, celebramos la movilidad permanente, el nomadismo trabajar en cualquier lugar gracias a la tecnología, pero donde «en verdad no todos pueden escapar a la exigencia de disponibilidad constante, la vigilancia de quienes te recuerdan que perteneces a una empresa y un lugar aunque estés en otra ciudad u otro país». En sus palabras: «Te regalan también la posibilidad de que el jefe te llame a las 11 de la noche y te encargue un trabajo de urgencia».

En un mundo de conexiones rápidas, donde estar siempre *online* es un deseo y a la vez una exigencia casi de *status*, la pregunta entonces es: «¿Dónde está el verdadero poder: en conectarse velozmente y con muchos, o en la posibilidad de desconectarse?».

Me respondo que, por ahora, prefiero poder desconectarme. Dejo entonces al reloj preso en su celda, su caja. La observo otra vez: si el reloj me hablara, su sonido sería un coro de sirenas, como las que tentaban a Ulises y sus navegantes y lo obligaban a amarrarse al mástil de su barco y a tapar con cera sus oídos para no sucumbir ante ellas.

La tecnología tiene un encanto similar. Nos propone vivir mejor, hacer todo más rápido, mantenernos al tanto de cada novedad, estar cerca de conocidos y desconocidos, divertirnos saltando de pantalla a pantalla. Pero, también, nos pide demasiado.

Un teléfono móvil o una computadora que nos resuelve ciertamente muchos aspectos de la vida también nos pide que le ofrendemos una parte de ella. Para que

los aparatos, las aplicaciones y los programas funcionen, debemos abrirnos ante ellos, ceder nuestros datos e información personal. Desde que encendemos la computadora, dependiendo del sistema operativo que elijamos, cedemos a su fabricante y a sus programas asociados determinada información.

Cuando navegamos en internet, el buscador que utilizamos va monitoreando y guardando nuestras preferencias: desde lo que tipeamos, los avisos sobre los que hacemos clic, las páginas que visitamos, las aplicaciones que utilizamos, el lugar en donde estamos haciendo esa pesquisa. Cuando usamos nuestros celulares, las aplicaciones registran a través del GPS nuestra ubicación, nos piden acceder a los datos de nuestras llamadas, contactos, preferencias de búsquedas, compras, fotos, música. Cuando utilizamos redes sociales, cada paso que damos va dejando también nuestras preferencias: qué páginas nos gustan, qué comentarios y a qué fotos les damos «me gusta» (*like*), con qué marcas y personas interactuamos. Nuestras huellas digitales van quedando desperdigadas en el camino, pero muchas veces no somos conscientes de que las vamos dejando. Y otra veces, sabemos que eso sucede, pero preferimos no verlo. Entonces con un movimiento certero del mouse le damos *aceptar* a los términos y condiciones de todos los productos, servicios, aplicaciones y redes sociales sin leerlos. La tentación de llegar rápido a utilizarlos, a que nos resuelvan un problema, nos hagan algo más fácil, nos diviertan o nos permita encontrarnos con otros es más fuerte.

El problema es que los datos que vamos cediendo a nuestro paso no quedan dentro del objeto que estamos utilizando —un teléfono celular, una tableta, una computadora—. Tampoco se dispersan en el éter de la Red, ni en esa nube mágica donde las empresas nos hacen creer que se almacena la información. Cada rastro digital queda en manos de empresas, en sus granjas de servidores, compañías que construyeron esos objetos con programas y aplicaciones que recolectan esos datos. Nuestras huellas son el oro de esas corporaciones: miles de millones de elecciones de personas alrededor del mundo que les dan a las empresas una base de datos actualizada en tiempo real cada vez que nos tentamos con un «me gusta», cada vez que buscamos un producto para comprar o para saber qué piensan otros que lo adquirieron, cuando completamos un perfil con nuestras preferencias en una página o una aplicación de citas, cuando usamos una red social para opinar, chatear e interactuar con otros. A las empresas que inventaron esos programas —que no son más que conjuntos organizados de personas— no les importa lo que pensemos o cómo seamos: les importa lo que hacemos y lo que consumimos.

Los objetivos de recolectar nuestros datos *online* no son siempre los mismos, pero están relacionados. Algunos pueden querer tenerlos para dañarnos: robar una identidad, cometer todo tipo de delitos, entrar en nuestras cuentas, ver lo que hacemos por razones espurias. Otros lo hacen con intenciones de vigilancia y monitoreo: Estados de todos los países utilizan los pasos dados por millones de personas en la Red para conocer más de nosotros, para recopilar esa información y

transformarla en un insumo de inteligencia con distintos fines. Y, también, están las empresas, a las cuales nuestros datos les interesan para construir perfiles cada vez más detallados de los consumidores, para ofrecernos lo que queremos comprar hoy o querremos tener mañana. Ese mercado de información personal es cada vez más grande, ayudado por todos los que, usando la Red, brindamos esa información, a veces siendo conscientes de los fines con los que será utilizada, y otras veces ignorándolo.

«El producto sos vos» es la frase más usada para explicar ese mecanismo por el cual internet evolucionó hasta convertirse en lo que es hoy: una gran máquina de obtener y procesar datos a través de servicios gratuitos para luego reutilizar toda esa información comercialmente. Si ayer buscamos en internet un pasaje a Nueva York, hoy nos ofrecerán el hotel. Pero aún más: si ayer nos interesó un pasaje y no lo compramos, hoy nos ofrecerán varias opciones más. Eso sí: serán probablemente más caros, porque el buscador habrá guardado una «*cookie*», un registro electrónico personalizado de nuestros caminos transitados por la Red que le dirá cuáles son nuestros intereses de consumo.

Si somos mujeres, jóvenes y a veces visitamos páginas de moda o belleza, nos tentarán con maquillajes o ropa. Pero si somos mujeres, jóvenes y visitamos blogs de autos, nos ofrecerán el modelo adecuado para nosotras. Si somos adolescentes, nos dirá qué película ver, qué concierto nos quiere allí. Y así para cada uno. Pero pueden ser también los sitios de noticias que visitamos y que «admiten *cookies*», capaces de seguir nuestro rastro de intereses: ¿nos gusta el deporte, el espectáculo, ambas cosas, o estamos interesados en la salud?

Pero además de usar la información para ofrecernos publicidad en forma directa, a través de avisos, los datos también se utilizan para hacer que los servicios que usamos en la Red nos ofrezcan «exactamente lo que queremos». Si dan con nuestro gusto, seguramente cliquearemos, es decir, compraremos. Un ejemplo es el cruce que realizan los buscadores (en nuestras computadoras o celulares) con la ubicación geolocalizada (a través del GPS, por ejemplo) que le ofrecemos voluntariamente. O con los *check-ins* que realizamos en distintos lugares con aplicaciones como Foursquare o Swarm («Ana hizo *check-in* en el restaurante chino Palitos», «Sebastián hizo *check-in* en el Caballito Shopping Center», leemos en nuestras redes sociales). Si mañana Ana está caminando por el barrio de Belgrano buscando un restaurante para comer con una amiga, abrirá su servicio de mapas y Palitos será la primera opción. Si mañana Sebastián busca dónde comprar un par de zapatillas nuevas, su *mail* recibirá una oferta imperdible para adquirirlas con su tarjeta de crédito que «casualmente» tendrá un 20 % de descuento en el *shopping* de Caballito.

Netflix es otro ejemplo de cómo los metadatos de internet se utilizan para detectar nuestros gustos y, en este caso, transformarlos en nuevos productos, por ejemplo, series o películas. Cada vez que le decimos al servicio de video que nos gustó tal película, la compartimos con nuestros amigos en las redes sociales, la calificamos con

una estrellita o cinco, o simplemente buscamos «Kevin Spacey» para ver films de nuestro actor preferido, el servicio toma nota. También se nutre de lo que rastreamos en servicios de descargas «ilegales», como los de *torrents*, o de *streaming online*. De esas búsquedas también se obtienen datos según las preferencias de la gente en determinado mes, año, lugar en el mundo, edad, sexo. *House of Cards*, la serie dirigida por David Fincher, creada y producida íntegramente por Netflix, se nutrió de ese estudio de los gustos de sus suscriptores. Mal no le fue: la compañía ya acapara el 30 % del tráfico de internet de Estados Unidos y tiene 50 millones de suscriptores en el mundo**[188]**, y la serie va por su tercera temporada y ganó los premios más importantes de la industria del entretenimiento, entre ellos varios Globos de Oro y Premios Emmy.

Internet funciona como un escáner de preferencias, a medida que le damos (voluntaria o involuntariamente) nuestros datos a algunas grandes corporaciones que se encargan de analizar cada huella que dejamos, cobrar por publicidad a las empresas que quieren vendernos algo y de predecir lo que vamos a desear mañana. Entre esas enormes compañías están los buscadores como Google, Yahoo o Bing! (pero especialmente Google), las redes sociales (sobre todo Facebook, por su cantidad de usuarios), y toda una serie de aplicaciones que utilizamos en nuestros móviles y van captando nuestra información.

Las bases de datos que se van conformando con las preferencias de los usuarios son el insumo más preciado de las empresas, tanto para ofrecernos hoy productos o servicios como para diseñar los que querremos comprar en el futuro. El análisis de esa gran cantidad de información, o *big data***[189]**, es un área a la que las empresas, a través de departamentos de investigación y desarrollo, le dan cada vez más importancia. La célula básica de esa maquinaria somos nosotros, cómo nos movemos, nuestros gustos y preferencias. Y esos datos son valiosos. «En febrero de 2014 Facebook compró la empresa de mensajería WhatsApp por 19 mil millones de dólares. La cantidad de dinero mencionada puede cobrar cierto sentido si se la compara con los valores con que cotizan empresas como United Airlines (15 mil millones), Sony (17 mil millones) o Fiat Chrysler (12 mil millones). Estas tienen edificios, oficinas, fábricas, diseños, equipos de investigación y miles de trabajadores, pero valen menos que una aplicación, algunos servidores, una oficina y unos 50 empleados. ¿Qué estaba comprando Facebook realmente? La respuesta es: acceso a los cerca de 450 millones de usuarios de WhatsApp», explica el periodista Esteban Magnani**[190]**.

El mercado de los datos es inmenso. En 2002, por primera vez en la historia, los humanos tuvieron más información almacenada de manera digital que en soportes analógicos. Cinco años más tarde ya casi el 95 % de toda la información mundial era codificada digitalmente. Es decir, vivimos rodeados de datos, que nosotros mismos

producimos cada vez que mandamos un *mail*, posteamos en una red social, buscamos en internet.

Google genera alrededor de 25 petabytes nuevos de información por día (exactamente la misma cantidad de datos útiles generados por el LHC o Gran Colisionador de Hadrones en un año). En YouTube se sube una hora de videos nuevos por segundo. Hoy, en 2015, somos 6500 millones de habitantes, conectados a 6500 millones de equipos electrónicos. En 2020, seremos 8000 millones de personas con 150 mil millones de objetos conectados, y habrá 57 *bytes* de información (o 57 caracteres —letras, números, emoticones—) por cada grano de arena en el mundo. Todos esos objetos conectados realizan acciones. Y esas acciones generan datos que no solo circulan por la Red: esa información recorre cables con dueños y queda almacenada en servidores de empresas. Esa enorme masa de datos aumenta su valor a medida que crece en volumen. En 2012, era de 6 mil millones de dólares. En 2018, será de 48 mil millones.

El valor de la información varía según quién la utilice. Por un lado, existe un mercado negro de datos personales. Según un informe de la empresa de seguridad informática Symantec de principios de 2015, los precios rondaban, por ejemplo, entre los 2 y 12 dólares por cada mil seguidores de redes sociales, o los 70 y 150 dólares por un millón de direcciones de correo electrónico verificadas. Pero luego hay un gran mercado «legal» de datos donde las empresas invierten en acaparar y analizar información para, fundamentalmente, realizar ventas y ofrecer servicios. Cuando Facebook compró WhatsApp estaba adquiriendo, fundamentalmente, una base de datos de 450 millones de usuarios. En Estados Unidos, las grandes tiendas usan la información de sus clientes para vender productos cada vez mejor direccionados, también de acuerdo con los comportamientos de los usuarios en los sitios de comercio electrónico. En la Argentina, el 50 % de las empresas afirma realizar algún tipo de monitoreo sobre los datos de los consumidores *online*, y ese porcentaje crece a medida que procesar los datos es cada vez menos costoso y las tecnologías para realizarlo más accesibles a una mayor cantidad de empresas.

Cuando Edward Snowden reveló que la Agencia Nacional de Seguridad espiaba masivamente a los ciudadanos de Estados Unidos y el mundo, no solo descubrió públicamente lo que hacía esa agencia estatal. También mostró que otras empresas privadas cooperaban para interceptar las comunicaciones o accedían a algunos pedidos de vigilancia. Sin embargo, pocos pusieron el foco en las firmas privadas. La razón es sencilla: Google y otras empresas similares adquirieron un gran poder al resolvernos con sus servicios cosas importantes y útiles de nuestras vidas. También, invierten miles de millones en publicidad.

¿Somos todos tontos al dejar nuestros datos en manos de otros o de regalarlos a cambio de servicios gratuitos? No. Los beneficios existen. Pero cada uno de ellos también conlleva un peligro, una deuda: una cesión de datos.

A Instagram le damos nuestros datos a cambio de tomar fotografías, ponerles filtros y compartirlas. A Twitter le damos nuestra información de perfil, ubicación, gustos y amigos a cambio de conectarnos con otra gente, leer las noticias y opinar de cualquier cosa. A Foursquare le damos nuestra ubicación a cambio de compartir reseñas de lugares, restaurantes y decir que estuvimos allí. A Facebook le damos nuestros datos a cambio de demostrar lo geniales que somos, lo bien que la pasamos y ver lo que hacen los otros y lo geniales que son ellos también. A Amazon le damos los datos de lo que compramos y las opiniones sobre esos productos a cambio de encontrar el mayor supermercado del mundo y algunas buenas ofertas. A Medium o algunas plataformas de publicación de blogs les damos contenidos gratis a cambio de darnos exposición pública. A Google le damos nuestros datos para vendernos cosas y que otros nos vendan más cosas a cambio de tener *mail*, usar Google Docs, hacer búsquedas, usar su navegador Chrome, sus teléfonos Android, su plataforma Blogger, su sitio de videos YouTube, su calendario, sus mapas. Damos, damos, damos. Somos eternos donantes de datos.

Mientras aceptamos estos intercambios, estas empresas ganan dinero. Mucho. Facebook sin usuarios no sería Facebook, y Mark Zuckerberg, su dueño, no estaría en el puesto 16 de los hombres más ricos del mundo[191]. Con más de 1350 millones de usuarios activos (en octubre de 2014) la empresa tiene un valor de más de 100 mil millones de dólares. ¿Dónde reside este valor? En nosotros, los usuarios: cada vez que agregamos un amigo, posteamos un comentario, una nota, o una foto, generamos información, es decir, más valor. Lo mismo sucede con Google, la empresa de publicidad más grande del mundo, basada en que todos dejamos nuestras huellas de datos cuando usamos su buscador, el *mail*, los mapas o los documentos. En el mercado de los datos, como ocurre con otros mercados de la tecnología, esas ganancias también se la llevan unas pocas, grandes y súperricas empresas.

El tecnólogo y escritor Jaron Lanier llama a este esquema «el modelo de negocios del canto de sirenas[192]». Según él, consiste en que estas pocas compañías «se quedan con toda la información posible y utilizan computadoras muy poderosas para obtener beneficios gigantes» en un formato que funciona haciendo que la gente les dé sus datos sin un beneficio monetario, sacándoselos subrepticiamente. Las empresas siempre ganan, nunca corren riesgos. Manejando esos detalles, pueden predecir las tendencias que tomarán las personas. «Por ejemplo, una compañía de seguros puede utilizar una gran cantidad de datos para solamente asegurar a quienes no vayan a enfermarse. El problema es que pueden hacerlo si tienen grandes computadoras para procesarlos. El resto deberá pagar por el riesgo». Para Lanier, el modelo funciona de manera brillante a corto plazo, es decir, en nuestra era, donde las grandes compañías como Google o Facebook se enriquecen, mientras siguen sumando servicios y personas a sus negocios. El problema es que, a largo plazo, esto nos lleva a otro problema de concentración del mercado de la tecnología. Y como la tecnología es cada vez más ubicua, no podemos escapar de ella para ninguna acción de nuestras

vidas y tampoco podremos escapar del poder de estas empresas. Aún más: las corporaciones como Google tienen planes para llegar a cada vez más actividades y negocios: desde fabricar autos y ser dueños de la flota de drones más grandes del mundo hasta predecir las enfermedades futuras a partir de las palabras que la gente tipea en su buscador[193].

Para Lanier, la última y también grave consecuencia de este modelo ya no es solo tecnológica. Es política y social. Porque estamos dando a estas pocas compañías el control de nuestro futuro. Pero también una serie infinita de negocios que hasta ahora están repartidos en otras empresas: las automotrices fabrican autos en el mundo; las farmacéuticas, remedios; las editoriales, libros. Ninguna de ellas es pobre ni hace beneficencia. ¿Pero qué ocurrirá si Google, por ejemplo, se hace fuerte en otra serie de industrias? ¿Qué pasará si, con internet.org[194], Facebook se convierte, además de dueño de la red social más poblada del planeta, en el principal proveedor de conectividad del mundo? Algunos dirán: es la competencia, es el libre mercado, es el darwinismo aplicado a los negocios, que siempre existió e hizo crecer al capitalismo. Otros sostendrán: todo cambio de época temió que una nueva casta de privilegiados se hiciera de todos los beneficios del nuevo modelo. Es cierto. Pero también somos nosotros quienes, en este caso, estamos ayudando masivamente, aceptando la tecnología sin crítica, a que el problema sea más que una decisión individual y se convierta en una cuestión colectiva.

¿Cómo contribuimos a incrementar este problema? Hay tres intercambios que, usados como ejemplos[195], pueden ofrecernos una nueva conciencia sobre el poder que dejamos en manos de otros.

El intercambio Google.
Servicios útiles y «gratuitos» a cambio de publicidad.

Google llegó a dominar internet como Julio César dominó Roma. Antes de él (de César y de Google) había un estado de caos. Roma tenía líderes débiles e ineficaces que no se ganaban el apoyo del pueblo ni lograban gobernar la ciudad. La Red, por su parte, era una colección de documentos asociados entre sí, pero desordenados, donde era imposible separar lo valioso de lo insignificante, lo cierto y lo falso. En medio de esa internet anárquica llegó Google. El 27 de septiembre de 1998, desde California, presentó un motor de búsqueda simple que clasificó el caos para los usuarios y dio el primer paso con el que sentó las bases de su actual imperio. El motor de búsqueda era limpio, puro y simple. No aceptaba dinero para situar una página adelante de otra en una búsqueda. El sitio más mencionado era el más relevante según los usuarios. Y lo mejor: funcionaba bien, cumplía su rol de editor en un mundo de anarquía. El secreto era que su técnica de búsqueda imitaba el modo en que el cerebro humano recuerda la

información. Fue fácil adoptarlo porque entró en nuestra mente como una herramienta más, como una extensión de nuestros pensamientos. Desde allí, buscar es *googlear*, conocer es *googlear*, recordar es… *googlear*.

A partir de ese primer paso, Google construyó su imperio. Con esa metáfora histórica, Siva Vaidhyanathan, un analista de medios que escribe en las publicaciones más prestigiosas del mundo, sienta su tesis de *La googlización de todo*[196], un libro donde explica cómo llegamos a darle a la empresa de Sergei Brin y Larry Page[197] el control de nuestras vidas, casi sin percibirlo, pero con motivos que no se explican solo por maldad o codicia capitalista. «Google domina la *Word Wide Web*. Pero jamás se llevó a cabo una votación para elegir quién la gobernaría. Ninguna entidad nombró a Google su representante, procónsul o virrey. Esta compañía llenó sencillamente el vacío cuando no había ninguna otra autoridad», dice Vaidhyanathan, que no considera a la empresa ni buena ni mala, sino que busca desentrañar cuánto de sus reglas moldean hoy nuestras vidas, al menos para conocer esas implicancias. «Ahora permitimos a la compañía determinar qué es importante, relevante y cierto en la web y en el mundo. Confiamos en Google e, incluso, creemos que actúa en nuestro beneficio».

Google ocupó un lugar. Lo hizo bien. Se convirtió en la empresa más eficiente de la Red. Su enorme poder no es casual. Sin embargo, como todo dominio que crece en un terreno de necesidad y expande sus tentáculos planetariamente, sus riesgos también pueden ser importantes.

Según Vaidhyanathan, la *googlización* de nuestro mundo afecta tres grandes áreas de interés y de la conducta humana. El primero es el «nosotros»: cómo Google influye en la información, los hábitos, las opiniones y los juicios personales. El segundo es el «mundo»: la aceptación de un tipo de vigilancia parecida a un «imperialismo infraestructural», es decir, una empresa que sabe, mediante nuestro uso de la tecnología, prácticamente todo lo que sucede en el mundo, que tiene un mapa de información capaz de predecir enfermedades, guerras, gustos musicales, decisiones políticas. Y todo eso lo hace desde Mountain View, una ciudad del condado de Santa Clara, California, que es la sede mundial del poder: allí también tienen sus oficinas Adobe, AOL, Facebook, Linkedin, Microsoft, Nokia, Red Hat, Symantec, VeriSign, entre otras. En esos cuarteles generales, Google posee una red de información que haría las fantasías de cualquier jefe del ejército del planeta: fotos de cada rincón del mundo, los datos —demográficamente segmentados— de cada persona que utiliza sus servicios, la información —en tiempo real, también en un mapa preciso— de qué le importa a la gente en determinado momento a partir de las búsquedas. Su tercer dominio es «el conocimiento»: Google tiene efectos poderosos sobre el uso del enorme conjunto de saberes acumulados en libros, bases de datos en línea y la Red.

¿Cómo llegamos a darle este dominio generalizado de nuestras vidas? Cediendo partes crecientes de nuestro uso de internet a servicios como Gmail, YouTube,

Google Maps, y las más de 150 empresas y aplicaciones que conforman su reino. La consecuencia es que en un tiempo (si ya no es así) la empresa estará a punto de volverse indistinguible de la internet misma. Pero como decía Spiderman (y antes había dicho Franklin Roosvelt): todo poder conlleva una gran responsabilidad. Y la eficiencia no nos permite ver que Google no es solo virtudes. Lo dice Vaidhyanathan: «Resulta obvio que Google mejora nuestra vida, facilita nuestros proyectos y reduce nuestro mundo que no tomamos en cuenta los costos, riesgos, opciones y consecuencias duraderas de la optimista aceptación que le otorgamos». Por eso, dice el autor: «Cuestionar el papel de Google en nuestra vida y la fe que le tenemos no es fácil. Google hace mucho bien y poco daño a la mayoría de la gente».

Junto con el bien, la compañía de Mountain View se transformó en el principal filtro del universo. El problema es que no es un cristal transparente, sino más bien un anteojo con graduaciones que altera lo que creemos cierto o importante. Es un espejo que nos devuelve respuestas a nuestras preguntas, pero antes las clasifica, desde una visión del mundo: aquella que construyeron un grupo de hombres y mujeres desde un lugar de California.

Pero la respuesta no es solo técnica. Es —otra vez, como en las guerras de internet— económica.

Google es una compañía de publicidad. La más grande del mundo. Su modelo de negocios reside en tener la información más actualizada de sus usuarios —es decir, de nosotros—, que somos a su vez consumidores en miles de otros sitios. Le interesa saber no solo qué hacemos, qué nos gusta y qué compramos hoy, sino qué vamos a querer hacer, qué nos va a gustar y por qué vamos a estar dispuestos a pagar mañana. Nos parece que la televisión, obligándonos a ver una publicidad en el corte, es una forma antigua de vendernos cosas y por eso apelamos al *zapping*. Pero Google lo hace todo el tiempo, ofreciéndonos y vendiéndonos lo que necesitamos (y lo que no) sin que seamos tan conscientes de ello.

El modelo de negocios de internet se basa en la publicidad: en miles de millones de dólares[198] que se invierten para vincular a usuarios con perfiles determinados con las marcas o los productos con los que podrían estar interesados. Para eso, las empresas que venden esos anuncios, principalmente Google que controla un tercio de toda la publicidad digital del mundo y más de la mitad de móviles[199], tienen que conocernos. Cuantos más detalles sepan de nosotros más eficiente será su negocio y más dinero podrán ganar. Los ingresos de Google, de hecho, están compuestos en un 91 % por ganancias de publicidad.

En internet todo puede medirse: si hicimos clic en un anuncio, si después de hacer clic comparamos entre dos productos y si finalmente compramos alguno. Cada paso está monitoreado. Tanto, que si ayer no nos decidimos entre un hotel u otro, mañana, sin recordar que ayer pensamos en el alojamiento de nuestras vacaciones, esa oferta de hoteles (o de otros) volverá. Google le cobra a las empresas por saber qué estamos buscando hoy, pero también porque tiene la información de lo que buscamos ayer y

los sitios que visitamos, que probablemente le dará las claves de lo que buscaremos mañana. Para hacerlo, estas compañías (Google, Yahoo, Facebook) tienen que invadir nuestra privacidad. No existe otra forma de hacerlo. Pedirles que no lo hagan sería reclamarles algo imposible: que cambien el modelo de negocios que les hizo ganar 60 mil millones de dólares en 2013 (siete millones de dólares por hora, 168 mil por segundo) y que sus dueños, Sergei Brin y Larry Page, abandonen la lista de hombres más ricos del mundo, con casi 30 mil millones de dólares en su cuenta bancaria, cada uno.

¿Qué sabe Google de nosotros? Lo que quiere saber: qué nos interesa, qué necesitamos y en qué creemos (política, religión, espiritualidad). Lo hace a través de algunos de sus servicios: las búsquedas de Google, el navegador Chrome, el servicio de correo electrónico Gmail, los avisos publicitarios (Google Ads). Google sabe lo que hacemos *online*: dónde usamos la computadora, qué escribimos y leemos, qué miramos. Para eso tiene, además de los servicios principales, otros como Google News (una sección de noticias curadas por sus editores), la no tan popular red social Google+, Book Search (para buscar libros), Double Click (una empresa de publicidad), Google Docs (un archivo y repositorio de todo tipo de documentos, que además se pueden editar y compartir en línea) y las plataformas Blogger (de blogs), YouTube (de videos) y Google TV (una plataforma de televisión inteligente).

Google puede localizarnos: sabe dónde estuvimos, dónde queremos ir, dónde trabajamos o nos encontramos a tomar un café, dónde vivimos y con quién nos comunicamos. A través de las búsquedas o usando su navegador, por nuestros *mails*, por los chats (Hangouts), por lo que compartimos en Google+, por su servicio Street View, por el Calendario donde marcamos las reuniones a las que iremos y con quién iremos, por sus Mapas, al usar las funciones de geolocalización de Android y a través de su aplicación Waze (de tráfico y navegación). También qué decimos, a quién le hablamos, cómo es nuestra voz, qué idioma hablamos, cuántos *mails* enviamos y con quién, a qué días y horas lo hacemos, y qué decimos en esos *mails*. Sabe, además, lo que compramos, cuánto gastamos y cuándo lo hacemos, a través de servicios como Google Checkout, Wallet y Shopping.

Si usamos un teléfono Android, también puede acceder a nuestra lista de llamadas, mensajes y búsquedas *online*. Además, guarda los datos de nuestra IP (el número que identifica el dispositivo que nos está conectando a internet) por 9 meses y las *cookies*[200] por un año y medio, lo que le permite un tiempo más que extenso para analizar los metadatos. Aunque intentemos evitar el monitoreo y tengamos configuradas algunas herramientas de privacidad Google sabe de nosotros. Un ejercicio sencillo para demostrarlo es tipear en su navegador «Google's ad preferences tool» e ingresar a nuestro perfil. Allí veremos quiénes somos para el gran mercado de la publicidad. En mi caso, Google sabe que soy mujer, que tengo entre 35 y 44 años, que vivo en Buenos Aires, hablo español, y me gustan o interesan cosas como: las artes escénicas (sí: voy mucho al teatro), la informática y la electrónica (sí:

trabajo de esto, Google), la casa y el jardín (sí: suelo buscar recetas para curar a mis plantas de algunos males), las noticias del mundo (sí: también es mi trabajo), la música *rock*, urbana y hip-hop, la política, las series dramáticas (sí: si son series sobre política, mejor), la venta de entradas de eventos (sí: últimamente compré muchas entradas *online*), las universidades, los libros y la literatura (sí, Google, soy una intelectual), y los tratamientos capilares (no recuerdo por qué, pero si Google lo dice, debo haber buscado algo para mi pelo).

Google es una red de compañías entre que hay más de 150 empresas[201] que fue comprando en la última década y que, asociadas entre sí, consiguen que casi nada de lo que hacemos quede por fuera de su dominio porque cubren todos los aspectos conectados de la vida de cualquier persona del mundo. Expandirse a nuestros cuerpos y ofrecernos conexión permanente para que nunca dejemos de conectarnos a sus servicios son los próximos pasos de la gran compañía. Así lo demuestran el desarrollo de objetos como Google Glass (los anteojos inteligentes que buscan reemplazar a los *smartphones*), programas como Behavio, que permite a las computadoras entender y reaccionar a los comportamientos de los usuarios y una serie de instalaciones y máquinas para ofrecer internet —directamente, sin recurrir a otros proveedores—, como los desarrollos que lleva a cabo Google Fiber (fibra óptica de altísima velocidad, 100 veces más que el promedio del mercado, en grandes ciudades), los drones de Titan Aerospace (para proveer internet en áreas de baja cobertura) o Loon (globos aerostáticos para dar conexión en áreas alejadas).

Con ellos, los servicios de Google estarán cada vez más interconectados con otros objetos para que la compañía se transforme en nuestra infraestructura digital, tan indistinguible como el aire que nos rodea. Ya hoy podemos verlo: estamos esperando el tren, chequeamos el horario en que pasa en nuestro teléfono o reloj inteligente, miramos el *mail* de nuestro jefe, aceptamos una invitación a una reunión, vemos la lista de cosas a comprar antes de llegar a casa y las noticias de la tarde para estar al corriente en la próxima cena con amigos. Google es nuestro reloj, nuestro editor de noticias, nuestra secretaria, nuestra mascota. Todo lo que necesitamos él lo sabe. Tal vez, incluso, lo que no teníamos ganas de conocer o de recordar.

La *googlización* del mundo tiene dos grandes consecuencias. La primera: convertirnos en productos, ignorando el verdadero alcance de lo que la compañía conoce sobre nosotros. La segunda —menos tangible pero igualmente vital para nuestro futuro— es que impone un mundo cuyas opciones se limitan y deciden desde las oficinas de la gran corporación. Ambos problemas responden a la misma causa, que está en el origen del negocio de Google: la recolección masiva de información y su administración.

La primera consecuencia está asociada con la cantidad de datos masivos que Google maneja de nosotros. Y a que en esa vastedad de detalles se juega una parte de nuestra privacidad. «En su núcleo, las compañías como Google están en el mismo negocio que la NSA. Recolectan una gran cantidad de información sobre la gente, la

guardan, la integran y la usan para predecir comportamientos individuales y colectivos, que luego pueden vender a publicistas y otros», escribió Julian Assange[202] al impulsar, en 2014, su cruzada contra la corporación liderada por Eric Schmidt. Según el líder de WikiLeaks, esta similitud convirtió a Google en el socio natural de la NSA e hizo que fuera colaboradora del megaprograma de espionaje Prism. «Google es más poderoso que la Iglesia», dijo Assange en su recorrido virtual por el mundo para presentar *Cuando Google encontró a WikiLeaks*[203], donde, además de demostrar que lo que parece gratis no lo es tanto, también en ese mecanismo hay prácticas que cuestionaríamos a los poderes del Estado pero muchas veces dejamos pasar cuando son obra de las compañías privadas.

Como afirma el tecnólogo Evgeny Morozov, el éxito de Google consiste en que su sistema es cada vez más ubicuo: llena cada espacio de nuestra vida cotidiana (nos manda una alerta para salir de casa media hora antes de la próxima reunión de trabajo, nos avisa que nuestro último turno con el médico fue hace un año, nos muestra el nuevo restaurante del barrio porque el último mes nuestro GPS nos llevó muchas veces a comer por allí). El problema, afirma Morozov, es que «somos demasiado mezquinos para no usar servicios gratuitos subsidiados por publicidad». El peligro es que con esto le damos, enceguecidos por sus soluciones mágicas, un inmenso reservorio de datos que lo alimenta para transformarlo en un animal cada vez más grande. Y allí reside su poder hipnótico para la economía y la política: en sus bases de datos se puede saber tanto de la gente (de nosotros) que la tentación de tener a la compañía como aliada es inmensa. Sin embargo, en el medio queda atrapada nuestra privacidad, o al menos nuestra opción de decidir quiénes tienen acceso a esa información.

Mientras tanto, para Eric Schmidt, el tema es sencillo: «Si tenés algo que no querés que otro sepa tal vez no deberías estar haciéndolo en primer lugar. Si realmente querés tener ese tipo de privacidad, la realidad es que los buscadores —incluido Google— retienen esa información por un tiempo». Su declaración recurre a una falacia repetida: «La gente inocente no tiene nada que esconder». Pero el problema no es si somos inocentes o culpables, sino algo previo: la privacidad importa por sí misma, porque es un derecho como usuarios y como ciudadanos. Es la base para la libertad, para expresarnos, para opinar. Si supiéramos que todo lo que hacemos va a ser visto por todos no actuaríamos de la misma forma.

La segunda consecuencia de la *googlización* está relacionada con el «orden del mundo» que nos ofrece la compañía y que hace que nuestro ecosistema se vea cada vez más limitado por las búsquedas, opciones y preferencias de lo que hicimos una hora, un día o un año antes en internet. Nuestros perfiles nos condenan. Somos lo que fuimos antes y, en el futuro, cuando queramos descubrir algo nuevo por fuera de lo que ya venimos eligiendo será gradualmente más difícil. Así lo advierte la periodista inglesa Aleks Krotoski cuando habla del fin de la serendipia, una palabra que significa la capacidad de descubrir algo accidentalmente, por casualidad, mientras

estábamos buscando otra cosa. Gran parte del progreso humano, creativo, o de las ciencias, se produce por efecto de estos hallazgos inesperados. Pero, para que suceda, tenemos que tener la capacidad de olvidar, reinventar, salirnos de las fronteras previstas. «Eric Schmidt, CEO de Google, declaró que quería que su empresa fuera no solo un motor de búsqueda sino un motor de serendipia, es decir, que pudiera predecir lo que la gente iba a preguntarse. ¡Y me pareció escalofriante! Porque no se puede predecir. Es un fenómeno individual, que se produce por accidente, y que termina teniendo valor. Por eso hay que reclamar la serendipia y cuidarla de que sea totalmente direccionada por la tecnología: porque es importante para el progreso de la sociedad», me dijo Krotoski en su paso por Buenos Aires[204].

Existen miles de ejemplos sobre cómo el mundo se achica si le damos todo el poder a las mismas manos. Uno es la construcción de los mapas de Google y cómo ella afectará el espacio público tal como lo conocíamos, en el futuro. Pero, más aún, sobre cómo esa lógica, al limitar nuestras opciones, nos convierte en personas más previsibles y al mundo en un lugar con menos capacidad de cambio (ni que hablar de grandes revoluciones). Según Morozov, la cartografía que nos propone la empresa es profundamente conservadora: «Ya que la lógica publicitaria es su negocio principal, la compañía no está realmente interesada en introducir novedades radicales a nuestras vidas. Para tener éxito con los publicitarios necesita convencerlos de que las visiones de sus consumidores son exactas y pueden generar predicciones sobre adónde queremos ir (o, para ese objetivo, dónde queremos cliquear). La mejor forma de hacerlo es transformarnos en criaturas altamente previsibles, limitando de manera artificial nuestras elecciones[205]».

Otra forma de hacerlo, señala Morozov, es hacer que todos vayamos a los mismos lugares, recomendándonos lo que otros amigos visitaron en el mapa, informándonos las actividades de nuestros contactos de Google Plus, o sugiriéndonos esos restaurantes adonde otros fueron. Claro que los ofrecimientos no están construidos solo por lo que nuestros amigos eligieron, sino por una mezcla de esas preferencias ordenada por la publicidad que otros dueños de restaurantes o sus agencias de publicidad le pagan a la gran corporación para ser exhibidas como las mejores opciones. «Google prefiere un mundo en donde siempre vayamos a los tres mismos restaurantes, antes que en uno donde nuestras consecuencias sean difíciles de prever».

Morozov rescata una frase de Daniel Graf, el director de Google Maps para móviles: «Si mirás un mapa: ¿debería ser siempre igual para vos y para mí? No estoy seguro. Porque yo voy a lugares distintos que vos». Sin embargo, advierte Morozov, aunque es cierto que todos vamos a sitios diversos, la «personalización» debería tratarse justamente de eso: de que nuestro instinto, gustos o preferencias determinen adónde queremos ir mañana y la capacidad de que eso sea diferente de ayer. O que, si elegimos otro lugar, seamos conscientes de que ese ordenamiento del mundo está construido por un algoritmo que guio esa preferencia por nosotros, pero además la

filtró de acuerdo con criterios publicitarios, con los cuales, al mismo tiempo, una empresa está ganando dinero.

Además de lo comercial, Google está modificando la ciudad, nuestra concepción del paisaje urbano tal como lo conocemos: «En el mundo de Google, el espacio público es algo que se asienta entre nuestra casa y los restaurantes mejor posicionados por las críticas, y a los cuales morimos por ir». El problema, en el final de esa lógica, es que la visión del mundo limita el rol fundamental que tienen el desorden, el caos y la novedad en nuestra experiencia como habitantes de las ciudades.

Esa limitación de la novedad, de la sorpresa y de encontrar lo que no pensábamos también se ve limitada en el rol de la gran corporación como editora de las noticias, especialmente a través de su servicio Google News, que ordena, filtra y edita por nosotros las novedades del mundo. Esta guerra llegó incluso a los tribunales europeos, cuando diarios y revistas de ese continente pidieron que Google les pagara por enlazar sus contenidos, que aparecían en su herramienta noticiosa con un título de la nota y un breve párrafo de la misma. En respuesta, Google dijo que el objetivo de News era llevar tráfico hacia los medios de comunicación, y que esto los favorecía en términos de tráficos, ya que no tenía la intención de retener visitas y, al contrario, dirigir a los usuarios a las respectivas fuentes. Los diarios insistieron en que, aun así, Google debía pagarles, ya que ellos eran los que estaban produciendo en sus redacciones la información.

En junio de 2014, medios alemanes demandaron a Google, que estableció que solo iba a exhibir el título del artículo con un link a este, sin citar nada ni mostrar imágenes. Sin embargo, tres semanas más tarde, los diarios decidieron volver atrás, dando un permiso gratuito al buscador para que los citara otra vez. Según algunos estudios, el tráfico desde Google News había descendido un 80 %. El ejemplo es otro más de un servicio que, con su ubicuidad, genera una situación de monopolio, en este caso informativo. Si no pasa por Google, no lo vemos. Si no lo vemos, no existe. Pero si existe, Google gana dinero. El círculo parece difícil de evitar y tiene a todas las industrias en la disyuntiva: ¿sumarse al gran poder o luchar, al margen de él?

Para los usuarios la perspectiva es similar. El dilema, para nosotros, es si la solución se trata de dejar de usar Chrome, Gmail, Android, Google Maps o Google Drive cuando nos hacen, efectivamente, la vida más fácil. La respuesta es que no es necesario, pero sí lo es saber cuáles son las consecuencias que tienen estos intercambios diarios. En el caso de las redes sociales, se suma otra negociación que puede ser peligrosa. Y allí no es por la eficiencia, sino por aspectos emocionales: ver qué hacen los otros, mostrarnos, conocer personas, buscar amor, explotar el ego.

EL INTERCAMBIO FACEBOOK.

Mirar y ser mirados a cambio de saber qué nos gusta (y filtrar nuestro mundo).

El 1.º de diciembre de 2014, los muros de Facebook se poblaron de un mensaje misterioso que sin embargo todos pensaron que sería bueno compartir. Con terminología legal, los cuatro párrafos de la proclama, reclamaban que lo que cada uno publicaba desde ese momento en la red social era propiedad personal y que la empresa no tenía derechos sobre esos datos, fotos o textos. El pedido se basaba en que la compañía había optado por «incluir el *software* que permitirá el uso de mi información personal» y que, recurriendo al «código de la propiedad intelectual» cualquier uso que se hiciera de la información debía tener un consentimiento por escrito de su responsable. Entonces hacía un llamado: «Los que leen este texto pueden copiarlo y pegarlo en su muro de Facebook. Esto les permitirá ponerse bajo la protección de los derechos de autor. Por esta versión, le digo a Facebook que está estrictamente prohibido divulgar, copiar, distribuir, difundir, o tomar cualquier otra acción en mi contra sobre la base de este perfil y/o su contenido». Y adelantaba una sanción: «La violación de mi privacidad es castigada por la ley (UCC 1-308 1-308 1-103 y el Estatuto de Roma)». Se invitaba entonces a todos los usuarios a publicar el texto y al final se advertía: «Si usted no ha publicado esta declaración al menos una vez estará tácitamente permitiendo el uso de elementos como sus fotos, así como la información contenida en la actualización de su perfil».

Cada vez que alguien reproducía el texto en su perfil, yo pasaba del asombro o la sonrisa a la certeza de que, si tantas personas estaban seguras de que podían hacer ese reclamo a Facebook, era porque la mayoría de los usuarios no conocen las condiciones que aceptan para participar en las redes sociales. Nadie lee los términos y condiciones, pero además somos ingenuos en suponer que lo que dicen puede proteger algo de nuestra privacidad. Pero además, la multiplicación de esos cuatro párrafos dejaba en claro que las empresas que manejan las redes son muy exitosas en que creamos que, cuando participamos en ellas, todavía somos los dueños de nuestros datos. Que todos compartieran ese reclamo significaba que todavía no hay conciencia de que, al ser parte de Facebook, formamos parte de una máquina publicitaria donde nuestros datos construyen perfiles de consumidores para vendernos productos a través de la publicidad en su propia plataforma o en otras relacionadas. Pero, aún más: al estar en ellas integramos estudios sofisticados que se realizan con los datos que les ofrecemos a través de nuestro comportamiento *online*.

¿Qué sabe y puede hacer Facebook de nosotros cuando aceptamos sus términos y condiciones[206]? Sabe dónde estamos, a través de la ubicación de nuestro dispositivo móvil. Recolecta información que le damos a otras empresas del grupo Facebook como Instagram o WhatsApp. Comparte nuestros datos con servicios de publicidad, medición y análisis, aclarando que siempre es información «que no permitan la identificación personal». También, con proveedores de servicios, por ejemplo, los de

infraestructura técnica (los servidores donde se guardan los datos), aunque aclara que «estos socios deben cumplir estrictas obligaciones de confidencialidad». La red social recopila datos de pago como el número de nuestra tarjeta de crédito, la fecha de vencimiento, el código de seguridad y la información de facturación de pagos o transacciones realizadas a través de la empresa.

Facebook aclara que puede compartir nuestra información personal en respuesta a un requerimiento legal, como una orden de registro, orden judicial o citación de organismos, dentro o fuera de Estados Unidos. También puede acceder, conservar y compartir información cuando crea de buena fe que es necesario para evitar el fraude y otras actividades ilegales, para protegerse a ellos mismos o como parte de investigaciones gubernamentales. La compañía conserva información sobre las cuentas que se desactivan por incumplimiento de los términos de uso durante un año, como mínimo, para «evitar que se repitan conductas abusivas o infracciones a las condiciones de uso». Para sus usuarios, de cualquier parte del mundo, que quieran reclamarle algún aspecto de su política de privacidad, el domicilio de la empresa está fijado en Irlanda, en el número 4 de Gran Canal Square, en Dublín.

Facebook es, después de Google, el segundo sitio más visitado del mundo. Creado en 2004, hoy cuenta con 1350 millones de usuarios en el mundo, la misma cantidad de habitantes que el país más poblado: China. A ellos se le suman los 300 millones de usuarios de Instagram y los 600 millones de WhatsApp, dos empresas que adquirió en 2012 y 2014, respectivamente. El negocio de Facebook es acumular usuarios que utilicen activamente los servicios, lo cual le garantiza tener perfiles actualizados, saber de qué hablan, qué les gusta, con quién y sobre qué interactúan. Cuando Mark Zuckerberg creó la plataforma en su habitación de la Universidad de Harvard, sabía que una red donde los estudiantes pudieran coquetear y conocerse entre sí tenía que ser exitosa. Su invento superó ese objetivo y hoy también es una plataforma de expresión artística, política, un lugar de encuentro social, familiar y profesional. Pero su función primitiva sigue siendo la base de su éxito: Facebook se trata de que nos vean y ver a los otros.

En ese intercambio emocional Facebook tiene la razón de su éxito. Suponemos que nuestras acciones están siendo «vistas» por alguien más que nuestros contactos. Podemos intuir que al usar su servicio «gratuito» y hacer clic en sus publicidades la empresa está ganando dinero: 60 centavos de dólar (multiplicados por 1300 millones de usuarios que permanecen un promedio de 40 minutos diarios en la red, la ganancia es millonaria). Intuimos que nada de lo que allí sucede es del todo privado. Sin embargo, en la negociación, preferimos *aceptar* sus condiciones y olvidar —o ignorar — las consecuencias.

No es sencillo culpar a los usuarios de caer en este canto de sirenas. Los «términos y condiciones» de los sitios de internet, las constituciones que determinan los derechos y las obligaciones dentro de esos espacios virtuales, son algo relativamente nuevo (en 1998 solo el 14 % de las web contaban con políticas de

información). Pero, además, están construidos para proteger a los sitios, plataformas o aplicaciones, más que a los usuarios. Un estudio realizado por el escritor Marcus Moretti y el especialista en derechos digitales Michael Naughton sobre los 50 sitios más importantes de Estados Unidos determinó que, sumados, sus términos y condiciones ocuparían 145 641 palabras. Es decir, unas 250 carillas de Word. Pero, aún si los leyéramos, lo que encontraríamos serían una serie de precauciones legales para proteger a las empresas de juicios y multas, escritas con un lenguaje vago, para reducir sus riesgos. En el medio de esas palabras las empresas han ido introduciendo mecanismos que contribuyen a recabar información para la industria de la *big data*: hábitos de consumo, afiliaciones políticas, orientación sexual, creencias religiosas, historias médicas.

Aceptar los términos y condiciones de un sitio o una red social es lo mismo que firmar un contrato. Pero como requiere un paso tan sencillo como hacer clic no le damos la importancia necesaria. «Si Apple pusiera el texto completo de *Mi Lucha* de Hitler en los Términos de Servicio de iTunes igual lo aceptaríamos», bromeó el conductor y periodista norteamericano John Oliver[207]. Sin embargo, al hacerlo, estamos dando consenso a una situación en la que nos convertimos en consumidores no solo de ese sitio, sino de todo un sistema de publicidad y servicios relacionados. Ese es uno de los grandes riesgos: con solo decirnos que «otros sitios» usarán la información pueden hacer que sean muchos más. Por ejemplo, al aceptar las condiciones del sitio de noticias de *The Huffington Post* otras treinta y tres compañías tienen acceso a nuestros datos, según Disconect App[208], una aplicación que permite bloquear los servicios de recolección de información de terceros. De los 50 sitios investigados por Moretti y Naughton, 48 recolectan datos para otros. Solo nueve de ellos informan para quiénes. El resto, lo oculta a cada uno de sus usuarios que hace clic en *aceptar*.

Si quisiéramos leer los términos y condiciones de los sitios que usamos en un año tendríamos que dedicar entre 181 y 304 horas[209]. Y repetir este procedimiento todos los años, ya que la mayoría de los sitios renuevan sus condiciones. Desde las compañías esto es pura estrategia: si los textos son largos y aburridos, entonces los consumidores no se van a molestar en leerlos o cuestionarlos. Lo cierto es que, en todo sitio que nos ofrezca un producto o contenido gratuito, nuestros datos serán utilizados, desde Facebook hasta sitios de pornografía con millones de usuarios diarios, como Xvideos o RedTube, cuyas políticas de privacidad, si las leyéramos, nos harían pensar dos veces en el placer inmediato que ofrecen sus servicios.

Pero además de escribir textos complejos para explicar algo muy simple («usaremos tus datos para venderte cosas o para darles tus datos a otras empresas para que lo hagan») las compañías como Facebook también estudian, a través de equipos propios de *big data*, los comportamientos de sus usuarios. Del tamaño de un país tan grande como China, Facebook es el laboratorio humano del comportamiento humano más extenso y diverso con que los investigadores pueden soñar. Si además

esas personas permiten a la empresa que las estudien, el siguiente paso no debería sorprendernos.

Durante una semana de enero de 2012, el equipo de Facebook Data Science y un grupo de investigadores y científicos de la Universidad de Cornell llevaron adelante un estudio que luego fue publicado en la prestigiosa revista *Procedimientos de la Academia Nacional de Ciencias*. Tomaron a 700 mil usuarios y los dividieron en dos grupos. Al primero le alteraron el algoritmo para que recibiera actualizaciones positivas, basadas en un filtro de palabras relacionadas (feliz, alegría, bueno). Al segundo, para leer lo contrario: noticias negativas, imágenes de tragedias, frases con la palabra «no». Al terminar la semana tomaron nota de qué posteaban los usuarios de uno y otro grupo. El resultado fue obvio: quienes habían recibido estímulos positivos, publicaban cosas felices, y viceversa. El problema es que ninguna de las personas sometidas al estudio fue avisada —explícitamente— de que estaba siendo parte de él.

En junio de 2014, dos años después de la investigación, la experiencia se hizo pública. De inmediato, los medios, las redes sociales y otros científicos se lanzaron a criticarlo. Y Facebook tuvo que salir a dar explicaciones. «La investigación se realizó solamente durante una semana y ningún dato utilizado estaba ligado a una persona en particular», dijo Isabel Hernández, vocera de Facebook. La empresa también se defendió diciendo que solo se afectó al 0,04 % de los usuarios y que su intención era mejorar el servicio para mostrar contenido más relevante.

El problema es que Facebook podía hacer este estudio, ya que sus usuarios lo habían autorizado cuando daban *aceptar* a los 9 mil caracteres (3 carillas de Word) de sus términos y condiciones. En todo ese palabrerío, la empresa mencionaba dos veces la palabra «investigación», informándoles que podían ser parte de experimentos. Sin embargo, la revista *Forbes* reveló que la palabra «investigación» fue recién incluida en mayo de 2012, cinco meses después del estudio. Y la comunidad científica aclaró: existen reglas estrictas para que los participantes de un estudio brinden un consentimiento informado ante cada procedimiento. No existe algo así como un «consenso general».

Pero Facebook no solo hizo esta investigación. Su equipo de Data Science, un grupo de sociólogos e informáticos que se dedican a transformar la *big data* de la red en resultados sobre los comportamientos y las expectativas de los usuarios, trabaja «a plena luz del día», da entrevistas y publica sus estudios en los medios. Esta vez, en lugar de estudiar si los enamorados bajan su nivel de interacción cuando se ponen de novios (algo que también habían hecho), alteró emociones sin consentimiento previo, algo con hipotéticas consecuencias (la depresión incrementa el riesgo cardíaco un 5 %, por ejemplo). Cuando se conoció el estudio, el filósofo de la tecnología Jaron Lanier escribió en *The New York Times*: «Sería inimaginable que una empresa farmacéutica pudiera experimentar, aleatoriamente, con una droga, en cientos de miles de personas. Imaginen al investigador diciendo: “Yo no sabía si te iba a afectar y no te molesté para hacerlo”».

La red social fue tan lejos que el profesor de la Universidad de Cornell Jeff Hancock, coautor del estudio, admitió a la revista *The Atlantic*: «El algoritmo de Facebook es algo raro que la gente no entiende. No lo hemos discutido mucho como sociedad. Hay un tema de confianza alrededor de las tecnologías». El argumento de Hancock es que hasta sus propios alumnos no entienden cómo funciona ni siquiera el algoritmo de Google.

La falta de «objetividad» de Google, y también de Facebook, es un aspecto a veces olvidado, pero que también se relaciona con el manejo que las empresas realizan de nuestros datos. Un objetivo vital de ambas compañías es que permanezcamos la mayor cantidad de tiempo posible en sus ecosistemas. De esa forma, ellas se aseguran ganancias superiores. Pero, para lograrlo, necesitan alterar el mundo, es decir, mostrarnos lo que queremos ver (en términos de sus algoritmos, lo más «relevante») durante más tiempo, rodearnos de estímulos agradables o al menos no conflictivos.

Ese mecanismo detectó el escritor y activista Eli Parisier cuando un día, al ingresar a su muro de Facebook, comenzó a ver que los comentarios de sus contactos con ideología conservadora estaban desapareciendo durante el agitado debate por la nueva ley de salud que impulsaba el presidente Barack Obama esos días. Él, un declarado progresista político, podría haberse alegrado de no leer toda clase de opiniones contrarias a su ideología. Sin embargo, decidió investigar y descubrió que Facebook había estado analizando que él hacía más veces clic en los links de sus amigos progresistas, y que por lo tanto estos empezaban a aparecer más: si él tendía a actuar más ante ese estímulo, la red social quería que él viera más de ese contenido que del de los conservadores. El problema es que no le consultó si él estaba de acuerdo con esa edición «invisible» y algorítmica de su mundo. Pero Facebook lo había hecho, y puede hacerlo, a partir de nuestro consenso. Google también: prueben buscar una palabra y pídanle a uno o dos amigos que también la busquen y les manden una captura de pantalla de los resultados. Todos recibirán respuestas diferentes. La razón es que Google, Facebook y muchos otros sitios saben desde dónde buscamos, qué pensamos, qué nos gusta, qué edad, sexo, religión y orientación política tenemos. Si no, no sería posible que cada uno reciba un resultado distinto. «No hay más un Google estándar», dice Eli Parisier, que a partir de su descubrimiento escribió *The Filter Buble*[210], donde explica que este mecanismo no solo puede aplicarse a Google o Facebook, sino que es también utilizado por buscadores como Yahoo News o sitios de información como *The Huffington Post* o *The New York Times*.

El planteo de Parisier vuelve al problema de un mundo donde, a partir de los datos masivos que tienen las grandes empresa de tecnología sobre nosotros, el universo de lo que vemos, accedemos, leemos o podemos descubrir se reduce cada día a una serie de opciones más personalizadas pero también más restringidas. «La

Red, que iba a permitir un mayor debate, que iba a contribuir con la democracia, resultó convertirse en lo contrario», advierte el escritor.

El concepto de la burbuja de filtros que construimos cuando aceptamos el dominio de los algoritmos sobre nuestros datos no queda entonces solo en una decisión individual. Es, también, un problema colectivo. Pero requiere de algo fundamental: nuestro consenso. Al igual que con una democracia, primero se necesita que elijamos vivir en ella y quienes nos representarán. Luego, que aceptemos y cumplamos las reglas que la delimitan. En las redes sociales acontece algo parecido: son un espacio público donde lo que decimos o mostramos no solo puede verlo cualquiera, sino que además tiene relevancia para lo que nosotros mismos veremos en el futuro. La responsabilidad, en ese y otros ámbitos de la vida digital, es nuestra, como ciudadanos de las redes, un espacio más que habitamos.

Pero allí anida uno de los grandes conflictos: cómo aplicar la responsabilidad y el control cuando podemos tener en la mano un aparato que nos resuelva todo con un par de clics. Eso también sucede con los teléfonos móviles y sus aplicaciones, que bajamos y utilizamos sin preguntarnos demasiado a dónde van los datos que les damos a sus dueños.

EL INTERCAMBIO MÓVIL.
Llevar una computadora a todos lados a cambio de saber todo de nosotros.

En 2025, además de los 4700 millones de usuarios de internet, habrá 150 mil millones de objetos conectados a la Red[211]: computadoras, heladeras, televisores, autos, ropa, casas. De todos esos aparatos, los teléfonos celulares son los más universales. No solo todos tenemos uno, sino que además lo llevamos como una parte de nuestro cuerpo. Y a diferencia de la computadora, cuya función está quedando en el ámbito laboral, por nuestros móviles fluyen nuestros datos más personales. Por ellos circula la información que indica dónde estamos, con quién hablamos, qué buscamos, qué leemos, las imágenes, la música y los videos más íntimos. Entrar en nuestro teléfono es ingresar a nuestra vida y a nuestra mente.

Los celulares son el dispositivo de control perfecto de nuestra era. Sin embargo, aunque allí está todo sobre nosotros, les damos poca importancia a los datos privados que acumulan. Aún más: entendemos poco de cómo funcionan sus programas y aplicaciones. Saben más sobre nosotros que nosotros mismos, pero dejamos que ellos o sus fabricantes hagan lo que quieren. Instalamos, damos *aceptar*, los llenamos de datos. Solo si lo perdemos o nos lo roban nos volvemos, por un momento, conscientes de cuánto de nuestras vidas hay en ellos.

Iván Arce apoya una taza llena de café negro en una mesa larga de la sala de reuniones de la Fundación Manuel Sadosky. Allí dirige desde hace tres años el programa de Seguridad en las Tecnologías de Información y la Comunicación, que vincula empresas, universidades y el Estado para capacitar recursos humanos locales en seguridad informática. De remera grande y cómoda y pantalones pegados a sus piernas largas y flacas, Arce no da nada por cierto cuando habla: todo para él puede ser de otra manera; necesita cuestionar antes de responder. Sus veinte años de trabajo en seguridad informática —como cofundador y líder de tecnología de una de las empresas del rubro más importantes del mundo— contribuyen a esa forma de percibir el mundo, donde todo requiere una explicación y un testeo antes de convertirse en verdad.

Para Arce, que dedicó su vida a *hackear* sistemas para encontrar vulnerabilidades y arreglar fallas, la tecnología nunca es neutra: Además de cumplir su función puede servir para defender o atacar a quien la emplea. Él sabe cómo se hace una cosa y otra. Y nada de lo que hoy es una preocupación reciente para los usuarios comunes de la informática —la privacidad, el uso de los datos, la posibilidad de acceder a nuestra información— para él es nuevo.

Arce respira profundo entre las frases y habla como en una conferencia: con silencios, encadenando lógicamente sus pensamientos, con tiempo. Y va paso a paso, también, cuando le propongo desentrañar los mecanismos que hacen que los teléfonos celulares se conviertan en los aparatos que más pueden conocer nuestras vidas.

—Este celular con sistema operativo Android —el más común que tenemos hoy en Argentina— es como tener una computadora y un módem juntos. Adentro, tiene muchos microprocesadores, con distintos programas corriendo. Cada uno está hecho por un fabricante distinto: el del *hardware*, el que hace los microprocesadores, el que realiza los programas, el que los integra, el del sistema operativo y todos los que hacen las aplicaciones de tu celular.

—*Es decir, que cuando te comprás un celular ya estás interactuando con mucha gente*.

—Exacto. Una gran diversidad de gente que «metió mano» en diversos lugares. Todos los teléfonos integran distintos fabricantes y proveedores. Si yo soy un atacante malévolo que quiero poner algo para vigilar personas, puedo hacerlo trabajando en la empresa que hace los microprocesadores que se utilizan en los controladores de placa de red, por decirte algún componente. Pero, además, vos después te bajás cualquier aplicación que te gusta sin preguntar quién la hizo y encima le das *aceptar* a todos los términos y condiciones.

—*Pero Samsung, Motorola o cualquier fabricante de móviles, ¿no saben eso, no realizan controles de seguridad para que no suceda?*

—Pueden saberlo, pero es imposible controlar toda la cadena de proveedores. Son cientos. Y miles de versiones, modelos y variantes de aparatos y programas.

—¿*Por qué un fabricante de celulares querría acceder a tu teléfono*?

—Para leer todos los datos que tenés ahí y espiar toda tu información.

—¿*No se supone que quiere que confíes en su aparato para algo tan importante como comunicarte*?

—Puede tener un interés de negocios ilegítimos en hacerlo. Puede obtener un montón de información de los usuarios: qué hacen, cuáles son sus hábitos de uso y de consumo. Pero también puede tener un interés legítimo en rastrear tus hábitos de uso para mejorar el dispositivo: entonces necesita «ver» qué tipeás o cómo usás la pantalla. La línea que demarca lo que es legítimo de lo que es ilegítimo en términos de negocio es muy difusa. Pueden decir que están monitoreando usuarios para mejorar un *software* que usás. Pero también para armar perfiles para después venderles publicidad. O para darle esa información a algún gobierno que la pida. Cualquiera de las tres opciones es posible. ¿Qué hacés vos para verificar que nadie esté abusando de tu datos personales?

—*En principio, no confiar*.

—No confiar igual es dejarlo en manos de otros. Con la seguridad informática hay tres caminos: mitigar el riesgo, transferirlo o aceptarlo. Mitigar es tomar alguna acción concreta: por ejemplo, encriptar el teléfono, descargarte alguna aplicación para verificar si te están espiando, controlar qué hacen las aplicaciones que te bajaste, revisar qué permisos les diste. Transferir el riesgo al Estado o al fabricante es que, si te das cuenta que no están protegiendo tus datos, les avises o les pidas explicaciones de qué están haciendo con tu información. Eso también es ocuparse activamente del problema. Si no hacés ninguna de esas dos cosas, estás aceptando el riesgo. No hacer nada es aceptar.

—¿*Y qué deberíamos hacer los usuarios de celulares*?

—Las tres cosas. El problema es que demanda un esfuerzo importante. En un mundo ideal, todos los usuarios de teléfonos celulares deberían preocuparse por su privacidad, encriptar las comunicaciones, los contenidos de su teléfono, verificar que los fabricantes no hagan suciedades, no instalar aplicaciones inseguras, no hacer clic en *mails* que mandan personas desconocidas.

—*Después de las revelaciones de Snowden se comenzó a hablar mucho más de criptografía, de encriptar las comunicaciones*.

—Encriptar es una de las herramientas de la seguridad y la privacidad, sí. Hay herramientas como Silence Circle Text Secure, navegadores como Tor, una larga lista de herramientas. Pero no es lo único que hay que hacer. También tenés que asegurarte

de que tu computadora y tu celular sean seguros y de tener la disciplina para hacer las cosas bien siempre.

—*Y dedicarle mucho tiempo a hacer todo esto.*

—Sí. Si tu vida está en peligro si te capturan las comunicaciones, deberías destinarle tiempo. Pero, si no, también. De otra manera, aceptás las cosas como vienen dadas.

El mundo que describe Iván Arce podría ser uno en donde vivir con paranoia sería normal. Sin embargo, como sucede con cualquier peligro, el miedo no soluciona sus causas. Desde que Edward Snowden le mostró al mundo que los ciudadanos de su país y el planeta estaban siendo espiados sin control, la primera reacción fue el terror de saberse monitoreado. Luego sobrevino una etapa de debate y de difusión de herramientas que los ciudadanos podemos adoptar para proteger nuestras comunicaciones.

Una parte de esta ola también estuvo teñida de un «*marketing* de la privacidad», donde empresas lanzaron productos y servicios más seguros para plegarse a la preocupación por el cuidado de nuestros datos. Entre otros, figuran Blackphone, un teléfono móvil que protege los datos de sus clientes; Qlink.it, un servicio para encriptar mensajes; nuevas versiones del navegador Firefox con elementos para reducir el rastreo de información; o una nueva serie de descargas del ya mencionado Tor, que ofrece opciones para una navegación más segura. También se incrementaron las descargas de Telegram, el servicio de mensajería desarrollado en Rusia con mayores recursos de seguridad que WhatsApp. Este mensajero, algunos servicios de Google y Yahoo sumaron —después de las revelaciones de espionaje del programa Prism— herramientas de privacidad y seguridad. El mismo Snowden recomendó utilizar RedPhone y Signal, dos aplicaciones para cifrar las llamadas en Android e iOS (el sistema operativo de Apple), respectivamente. También, el uso de Text Secure, como alternativa a las aplicaciones de mensajería como WhatsApp y Telegram. Y preferir Spider Oak, un servicio de almacenamiento en línea para reemplazar a Dropbox, que había sido indicada como unas de las empresas en colaborar con la NSA. La lista de opciones, la mayoría de ellas basadas en *software* libre y desarrollos en los márgenes de las corporaciones, se multiplicó.

Organizaciones de derechos fundamentales en internet como Access Now y la Electronic Frontier Foundation (EFF), entre otras, publican y actualizan herramientas y aplicaciones que permiten una protección de la privacidad. La EFF tiene un Kit de Autodefensa contra el Monitoreo, en español, en ssd.eff.org/es, con tutoriales y materiales traducidos. Digital Defenders cuenta también con uno con distintos recursos para protegerse en digitaldefenders.org/digitalfirstaid/. Y el colectivo Tactical Technology también tiene su botiquín de primeros auxilios para proteger la privacidad en info.securityinabox.org/es. Cualquiera de estas herramientas,

actualizadas con frecuencia y usadas en conjunto (en la computadora, el teléfono, las comunicaciones, las aplicaciones), son útiles. Pierden su efecto si protegemos un dispositivo como el celular, pero luego, por ejemplo, sincronizamos el *mail* con una tableta y allí no protegemos las comunicaciones o usamos otro navegador.

Para Arce, no hay un sistema de seguridad perfecto, sino que existen usuarios con distintas necesidades a proteger.

—Lo más importante no es qué herramienta uses, sino la conciencia y la disciplina. Es generar un entorno seguro para vos, pero saber que vos formás parte de redes, donde no solo pueden espiarte a vos, sino a quienes tienen contacto con vos. Relajarte en tu seguridad puede tener consecuencias más o menos graves. Depende de qué sea relevante para vos y cuánto tiempo vas a dedicarle.

—*Por ejemplo, en tu caso, ¿cuáles son tus necesidades y cómo las protegés?*

—Yo no sincronizo mis cuentas, es decir, no conecto unas cuentas con otras. Solo mando mensajes de SMS y los encripto con Text Secure. No uso *mails* en el teléfono; solo lo hago en la computadora. No hago backups de contactos en la nube, y deshabilito backups automáticos. Si pierdo las cosas, es un riesgo, pero yo decido. Y hay cosas que estoy dispuesto a perder.

—*¿Por ejemplo*?

—No uso la mayoría de las redes sociales. Pero es lo que yo estoy dispuesto a hacer. Es como en la película *El Padrino*: a veces te querés salir de «un asunto» peligroso, pero después tenés que volver a entrar o alguien te hace volver a entrar y te lleva al peligro. Acá es lo mismo: es resistir esa ola que te lleva, saber que si no tenés esa disciplina vas a correr riesgos. Y bueno, tampoco estoy en el grupito de WhatsApp de los padres del jardín de mi hija: me pierdo de enterarme de cosas allí, pero las pregunto en la puerta cuando la voy a buscar.

—*Bueno, no estar en el grupito de WhatsApp de padres del jardín tal vez es una ventaja…*

—Sí, quizá es una ventaja secundaria de proteger mi privacidad —se ríe el experto en seguridad informática, y por un momento deja su seriedad de especialista para convertirse en un padre moderno, pero no lo suficiente como para perder el control de su privacidad.

El manejo de la privacidad y de nuestros datos será una de las guerras de internet más importantes del futuro. Lo será para reclamar a empresas y gobiernos que no nos espíen o que, si lo hacen, nos dejen saberlo. Las batallas serán por nuestros derechos: para decidir con quién compartimos nuestros datos, quiénes los manejan y controlan o de quién queremos protegernos.

También somos nosotros los que corremos, cada día, la frontera de lo privado. Queremos, reclamamos y actuamos para ver más de los otros. En 2014, cuando WhatsApp incorporó un ícono de «doble visto» en forma de tildes azules, muchos usuarios lo festejaron: ahora iban a poder saber cuándo sus mensajes eran leídos. Podían reclamar ser vistos o ser ignorados. Cuando eso sucedió, yo desactivé esa opción para que nadie pudiera ver si yo leía o no un mensaje, pero eso también implicaba que yo tampoco viera si los otros leían mis comunicaciones. A los pocos minutos de cambiar la configuración por una más privada, recibí un comentario:

—¿Por qué desactivaste el visto? ¿No te interesa ver si leen tus mensajes? —me reclamó un contacto de mi lista, con sinceridad.

—No, no me interesa. Bueno, en realidad a veces sí me interesa o me da curiosidad. Pero si el precio de saber si me leen es dejar abierta mi propia privacidad, prefiero no hacerlo.

La privacidad no siempre existió tal como la conocemos hoy. Es una idea de la modernidad, que se asentó cuando, con la revolución industrial, las ciudades crecieron sobre las áreas rurales. Al estar unos más cerca de otros necesitamos marcar límites. Hoy la consideramos algo que siempre existió, pero es, en verdad, una idea reciente en la sociedad. Al mismo tiempo, cuando estábamos acostumbrándonos a ella, el concepto de lo privado cambió a partir de la convivencia de la tecnología en cada aspecto de la vida. Hasta hace algunos años, incluso, pensábamos que internet podía ser un ámbito distinto de la «vida real». Que lo *offline* y lo *online* eran posibles de separar. Hoy, esa idea también quedó vieja: sabemos que ni son diferenciables ni tampoco el espacio de la Red es privado.

Sin embargo, todavía le reclamamos a lo *online* cierta privacidad. No reconocemos, tampoco, que en ese territorio existen dueños. Que quienes interactuamos allí lo hacemos bajo las reglas de otros: las empresas que controlan esos espacios.

El filósofo Darío Sztajnszrajber ocupa una mesa doble en la confitería Las Violetas, muy concurrida durante una mañana de marzo en que Buenos Aires recobra el ritmo del comienzo de clases. En nuestro rectángulo, rodeados de otros comensales que desayunan, leen el diario o trabajan, la conversación con el filósofo es privada. Pero ya nada garantiza que alguno de nosotros termine la charla y tuitee una frase que dijimos, alguien nos saque una foto y la suba a una red social o que nuestros teléfonos estén registrando todo al tiempo qué hablamos, sin darnos cuenta.

—¿La tecnología siempre implica control? ¿Siempre quien tiene mis datos tiene un poder sobre mí?

—Siempre hubo formas de control y de recabar la información casi total de las personas. Sucedió en diferentes momentos, con tecnologías distintas. No es la

primera vez que la tecnología genera control. Hoy, también, hay una relación simbiótica: hay más datos porque hay más tecnología y hay más tecnología porque hay más datos.

—*¿Por qué le reclamamos al Estado que no nos espíe, pero no parece molestarnos que lo hagan las empresas*?

—Hay parte de la sociedad que sigue creyendo en la transparencia del capitalismo y del liberalismo. Cuando no cuestionamos a Google, en realidad no cuestionamos al mercado. Pero sí cuestionamos al Estado porque, según la idea liberal, el Estado manipula la libertad individual.

—*Pero está la idea de que «tenemos menos privacidad», podemos ir por la calle y ser filmados por una cámara o que alguien nos saque una foto y la suba a una red social*.

—Es que todo está relacionado con el contexto en que se da. Esa idea, hace cincuenta años, no hubiera tenido sentido, porque no estaban dadas las condiciones materiales, tecnológicas, para que sucediera. Si lo analizamos sin ese contexto, siempre lo vamos a ver como una pérdida o una degradación. Yo me peleo con esas posturas que ven que el mundo actual es un mundo que está perdiendo ciertos valores. Porque los valores no existen; son una construcción de la época. Hoy las formas de privacidad se «transformaron», no diría que se «perdieron». Se transformaron, porque hay otras también.

—*Las categorías llegan después de los cambios*.

—Exacto. Las instituciones siempre llegan tarde y las categorías explicativas, peor. Nos cuesta entender cómo la revolución tecnológica va minando de raíz las categorías con las que venimos pensando una realidad material diferente. ¿Sirve seguir hablando de identidad o de privacidad, en el mundo de las redes? Yo digo que no. No en la forma en que definimos lo privado y lo público o definimos identidad, por los menos en el siglo XX. ¿Qué sería lo privado y lo público en una red? Volver a pensar categorías es lo que más nos cuesta. Me parece que el gran drama con las transformaciones tecnológicas es ese. Es algo que pasó siempre, pero ahora el cambio va mucho más rápido. Obvio que hay gente que necesita seguir pensando la realidad con algunas categorías de verdad. Pero también hay mucha gente que necesita seguir creyendo en Dios.

Las guerras de internet también se tratan de eso: de qué intercambios hacemos para convivir con unas tecnologías que alteran nuestros hábitos, nuestras relaciones con los demás y el control de nuestros derechos. Pero mientras negociamos esos límites en forma privada, también formamos parte una sociedad que va cambiando sus

formas. Y somos ciudadanos que construimos, con nuestras acciones, los derechos colectivos.

Las revelaciones sobre espionaje masivo que dio a conocer Edward Snowden en 2013 hicieron más visible un tema que ya preocupaba a especialistas en derechos de internet, académicos, gobiernos y activistas: quién controla nuestros datos y hasta donde la privacidad puede existir en la era digital.

En respuesta al problema, un grupo extremo propone dejar de usar internet porque estar en ella nunca es privado. En el otro extremo, están quienes la usan sin ningún cuidado: son aquellos que sostienen el argumento de que no tienen nada que esconder y, por lo tanto, nadie va a espiarlos. La tercera opción, que es la intermedia y más compleja de concretar, requiere compromiso y trabajo de nuestra parte: partir de la base de que nuestros datos ya no son privados y tomar algunas medidas al respecto, no solo como individuos aislados sino como parte de una sociedad.

En lo personal, el cuidado de nuestra privacidad con herramientas de encriptación, navegación anónima, el uso de sistemas operativos abiertos o productos que nos brinden información respecto de cómo están construidos o cómo manejan nuestros datos, son todas formas de ocuparnos del tema. Todas requieren tiempo, disciplina y compromiso. También que compartamos los conocimientos con otros, para generar el cambio y la adopción de esas herramientas por parte de quienes todavía no las utilizan. Sentarse un momento, una hora o incluso dos, con un amigo, un familiar o un colega, a explicarle cómo funcionan «las cosas» (en este caso, la tecnología) es un acto político, de expansión de derechos, porque permite ser más conscientes de lo que usamos y no adoptar soluciones empaquetadas por otros. Si cuando vamos al supermercado no compramos productos muy caros en señal de protesta, si reclamamos a nuestra comuna que reparen una vereda o salimos a pedir a una manifestación un cambio político, deberíamos también generar acciones concretas respecto de nuestro uso de la tecnología. Si no lo hacemos, estaremos dejando que las cosas sigan como están.

Mientras tanto, en el mundo, se proponen soluciones para enfrentar o lidiar con los temas de privacidad.

La primera es una respuesta económica y propone que, ya que de todas formas nuestros datos serán usados por las empresas, que ellas nos paguen por hacerlo. La empresa Datacoup[212], por ejemplo, se presenta como una plataforma donde podemos ofrecer todos los accesos a nuestras cuentas, redes sociales y aplicaciones, y ganar dinero para que se utilice la información que hoy en día esas compañías utilizan sin compensarnos por ello. Existe un movimiento a favor de esta opción que está creciendo en el mundo, sobre la base de «si me van a espiar, por lo menos páguenme». Sin embargo, es una decisión peligrosa, porque su cimiento es aceptar la recopilación masiva de información y legitimarla. Es como la prostitución legal: que sea en Ámsterdan, con profesionales del sexo y en lugares limpios, no hace que no sea una explotación del cuerpo de otro. Además, la solución incrementa la

desigualdad, porque no hace más que darle de comer al monstruo que se alimenta de los datos. Entonces, quienes más cuentas o datos tengan, ganarán más dinero, mientras que los que ya tienen menos, quedarán más al margen. Finalmente, tampoco resuelve qué pasaría con quienes no quieran vender sus datos a cambio del beneficio económico: ¿serán marginados de internet?

La segunda es la solución política, y es la que preferimos. Se trata de tomar a la privacidad no como un fin en sí mismo («la privacidad está bien porque sí»), sino como un medio para otro fin más importante: vivir en un sistema democrático, donde podamos optar. Sin espacios privados, donde un algoritmo no decida por nosotros si quiere monitorearnos, o donde estemos obligados a vender nuestros datos como mal menor a que igual los recolecten, no seremos ciudadanos completos. Para que las democracias sean realmente efectivas, necesitan que podamos negarnos a ciertas decisiones, que tengamos la capacidad de sabotear el sistema, de no aceptar las cosas tal como son dadas, sino cuestionarlas en caso de que estemos en desacuerdo con ellas. Si los aparatos y las aplicaciones nos proponen acompañarnos a todos lados, registrar nuestras pulsaciones, calorías, los lugares que visitamos y con quiénes conversamos, deberíamos también poder elegir entre otros que no lo hagan o prescindir de aquellos que lo hacen.

Esta opción no es fácil. Implica entender internet —y a la tecnología— sin ingenuidad. Significa no pedirle que resuelva todos los problemas por nosotros. Si dejamos que Google, nuestro proveedor de internet, los dueños de las redes sociales, las «nubes» donde guardamos los datos y los servicios de mensajería se encarguen de nuestras vidas porque es más fácil y nos ahorra tiempo, estamos cediendo un gran poder en sus manos. Es como elegir un presidente, un gobernador o un diputado y permitir que actúe sin control durante los cuatro años que dura su mandato. Es delegar todo en manos de otros para no ocuparnos nosotros. Ahora, si algo sale mal, ¿cómo reclamar después si no nos importó en su momento? Con la tecnología sucede lo mismo que con la representación política: ella siempre va a avanzar si la dejamos. La única forma de que no lo haga siempre para el mismo lugar (como otra forma de capitalismo concentrado) es entenderla, para ponerle límites, reclamarlos o construirlos colectivamente.

Desde este punto de vista político, la privacidad «en sí» no es el problema. Lo es, en cambio, el control de la privacidad. Quién monitorea mi información, cómo lo hace, con qué herramientas, informándome o no, son las preguntas que debemos hacernos. Porque allí —en reconocer a los poderes que controlan nuestros datos, cuánto ganan, para qué lo hacen— estaremos sabiendo más del mundo que nos rodea, en este caso en forma de tecnologías que deciden sobre nuestra vida.

Nuestros datos son más que unos y ceros. Son nuestras vidas, historias personales, lo que queremos, lo que soñamos. La privacidad depende de cada uno. Es una lucha política que requiere involucrarse. La otra opción es elegir por la eficiencia, los intercambios para hacer las cosas más fáciles o más rápidas, y olvidarnos de las

consecuencias. Si esa es la decisión, entonces será lógico entregar nuestros datos a las empresas que nos prometan que en sus manos obtendremos beneficios. Si lo hacemos, debemos saber que les estamos dejando ese lugar a ellos porque nos resulta costoso ocuparlo: porque no tenemos tiempo, porque no nos dan ganas, porque preferimos ocuparnos de otras cosas.

Esa opción, la de no ocuparnos, también es una elección política. No controlar nuestra privacidad y nuestros datos nosotros mismos implica cedernos a otros. En esa antipolítica, habrá otros que harán política o negocios con nuestra información. Sin embargo, existe otra alternativa, la misma que nos hace salir a la calle a reclamar por algo que nos preocupa o a defender algo que queremos. La misma que nos hace participar en nuestro consorcio, organización social o comunidad. En la tecnología y en las guerras de internet también hay —y habrá— batallas por pelear, territorios en disputa por defender. Depende de nosotros tomar las armas y salir a ocupar esos espacios.

Epílogo

Entender el poder, transformar internet

> «El mensaje que estoy tratando de enviar es que la tecnología es política, y que muchas de las decisiones que se parecen a las decisiones acerca de la tecnología en realidad no son en absoluto acerca de la tecnología. Son de política. Y necesitan ser examinadas tan de cerca como las decisiones sobre política».
>
> EVGENY MOROZOV.

A medida que avanzaba en la escritura de este libro se me hacía cada vez más presente la frase de un profesor de Economía Política con el que nos encontrábamos a leer *El Capital* de Marx los sábados a la tarde:

—A Marx le criticaban que no hubiera pensado en el concepto de capital como se desarrolló veinte años después. El tema es que se murió antes de poder pensarlo. Y de verlo —nos decía Néstor, con su barba larga, fumando un cigarrillo negro en el círculo de sillas de un bar.

Escribir sobre tecnología es siempre una carrera contra algo que va a cambiar mañana. Implica pisar sobre un terreno farragoso, que muta y que no podemos predecir. En cierta forma, vamos a *morir* o —en este caso, menos grave— a entregar un libro que correrá atrás de cosas, conflictos y objetos que están mutando.

A mí, en vez de darme miedo, esa carrera contra las transformaciones me parece fascinante.

El «periodismo de tecnología» *mainstream* adora hablar de lo nuevo. Tiene una excitación casi pornográfica en mostrarnos los aparatos (o *gadgets*, como le gusta llamarlos) apenas salen, si es posible «antes que otros», «antes de que lo veas en tu tienda favorita». Sin embargo, en esas maratones que se desatan por la novedad, lo que se alimenta no es más que la obsesión por el consumismo. Con ella, la tecnología se convierte en una cosa más que compramos para adquirir estatus, eficiencia, tiempo, diversión. El riesgo es que esa forma de ver y presentar el mundo nos convierte en esclavos de las máquinas. Y, aún peor, nos hace adoptarlas como a una religión: sin mirar quién las creó, qué nos proponen, quién gana dinero con ellas o si realmente las necesitamos.

Con esa idea empecé a escribir este libro que hoy termino. Pero, además, durante todo su camino lo construí con dos cualidades que creo que el periodismo está perdiendo: la curiosidad y la crítica.

La primera —la curiosidad— hizo que quisiera inmiscuirme adentro de la tecnología y no solo mirarla desde afuera. El ejercicio de mirar adentro de los cables, los servidores, las empresas, los dueños y los organismos que gestionan internet me descubrió algo fascinante: aunque para los usuarios es algo unívoco, omnipresente y casi mágico, la Red en su interior tiene muchos significados y genera miles de luchas. Internet y las tecnologías en general solo son algo «cerrado» para convertirse en productos que queramos comprar en una góndola o en un clic desde la computadora. Pero, vistas desde adentro, son heterogéneas, desordenadas y motivo de disputas feroces. A veces, esas peleas llegan a quienes usamos los aparatos. En ese momento, como sucedió por ejemplo con las revelaciones de Edward Snowden o algunas denuncias de Julian Assange, abrimos los ojos y por un breve instante tomamos conciencia de que internet es también un ámbito de la política. Internet no solo nos da poder a los usuarios, sino que su poder también puede ser motivo de disputa.

La segunda —la crítica— logró algo maravilloso en mi camino por descubrir internet: no quedarme elogiando sus virtudes ni volviéndome una apologista de sus defectos. Desde hace años, me horroriza la visión de los optimistas de la Red, aquellos que confían ciegamente en ella como instrumento democratizador y de progreso del mundo. Es obvio que no es así. Después de 25 años de *Word Wide Web*, si la ecuación fuera tan directa, en el mundo ya no habría desigualdades. Sin embargo, tampoco me interesa permanecer en el otro extremo, aquel que únicamente ve en internet una amenaza a las libertades, a la privacidad y a los derechos individuales. Pensarla así implica otro riesgo grave: resistirse al cambio. Ver en la tecnología nada más que destrucción implica otra cara de un individualismo que diluye los lazos sociales. Sé que algunas tecnologías restringen mi privacidad, pero dejar de usarlas me dejaría fuera de un mundo donde quiero vivir con otros, socialmente, para hacer algunas cosas que también me resultan importantes: expresarme, charlar de política, encontrarme con amigos.

No obstante, aunque también puedo pensar en la tecnología de forma positiva, el futuro de internet me preocupa. Por un motivo político: les estamos dando a unas pocas corporaciones que dominan nuestra vida en la Red un poder monumental. Google, Facebook, Yahoo, Apple, Microsoft, y algunas más con nombres menos conocidos pero igual de monopólicas, hoy dirigen nuestras vidas, a través de sus aparatos, programas y algoritmos. Lo hacen con la fuerza de gobiernos universales y omnipotentes. Mientras tanto, con ejércitos de publicidad y *marketing*, nos venden sus productos y servicios con un espíritu tan positivo que perdemos de vista sus consecuencias. Mientras que cuestionamos a los políticos que votamos, a este puñado de corporaciones les creemos *todo*. Como dice la investigadora Rebecca MacKinnon

—en una frase que me quedó grabada en la cabeza—: somos capaces de ver el poder en el mundo real, pero todavía no entendemos cómo opera en el mundo *online*.

El objetivo de este libro es ese: entender cómo opera el mundo *online*. Porque entender cualquier poder sirve para transformarlo. En el caso de internet y de la tecnología, somos tantos los usuarios que, si cada uno entendiera más cómo funciona, tendríamos una fuerza tremenda para defendernos de las nuevas dictaduras, monopolios y abusos que algunos de sus dueños están creando.

Hay algo que descubrí escribiendo este libro: que mi generación, la que comprende a los hombres y las mujeres que hoy tienen 35, es la que más se va a preocupar porque internet no mute en un animal horrible, en un gran animal fuera de control, como en las peores fantasías distópicas del mundo orwelliano. Me di cuenta de eso a medida que conocía y entrevistaba a los activistas por los derechos de internet que hoy levantan su voz en las redes sociales, en los medios de comunicación o en los encuentros políticos del mundo.

En América Latina, muchos de quienes hoy están trabajando por un mejor futuro de la Red también comparten mi historia. Son hijos de padres militantes en los 70, aquellos que vivieron en países bajo regímenes y personas que los controlaron hasta matarlos. No nacimos en sociedades libres; las vimos nacer.

En 1987, cuando yo tenía siete años, mi mamá me dejó al cuidado de mis abuelos. Ella se iba con mi papá a la Plaza de Mayo, «a defender a Alfonsín», es decir, a defender la democracia. Estaba ocurriendo un alzamiento militar de un grupo de poder que quería volver a instaurar una dictadura en Argentina. Antes de irse, mi mamá me dio un beso y me dijo que me quedara tranquila, que ella iba a regresar, pero que necesitaba salir a la calle a cuidar el país de los malos. Desde ese momento, supe que la política se construye con acciones, no con palabras. Que a veces hay que dejar la comodidad del sillón y tomar compromisos. Soy de esa generación que vivió la bisagra de un régimen sin libertad a otro más libre, que si no se defiende tampoco tiene valor.

Además, soy la primera generación que vivió las dos épocas: con y sin computadoras. A diferencia de los niños y jóvenes de hoy, cuando yo empecé a usarlas, todavía no eran aparatos que inundaban ubicuamente en nuestras vidas. Se prendían y se apagaban. Internet implicaba conectar y desconectar un cable. Salir a la calle no era ser visto por diez mil ojos. Cuando era adolescente, todavía podía darle a mi novio un beso a la vuelta de la esquina sin que una cámara me filmara para salir luego en una publicidad de Coca-Cola. Pero eso fue cambiando. Para bien, porque las máquinas hicieron algunos aspectos de la vida más fáciles y mejoraron la comunicación entre las personas. Y para mal, porque hoy estamos más controlados. Y porque desconectarse de la tecnología requiere disciplina y voluntad.

Para ser conscientes de lo bueno y lo malo de la tecnología hay un primer paso imprescindible: conocerla, desde su entramado y su poder. Esa es una tarea de nosotros, los periodistas (a secas: de tecnología, de política, o de ambas cosas, como

yo me considero). Internet también cambió la forma de hacer periodismo. Hoy hay muchas más herramientas para descubrir los hechos, a sus protagonistas y las distintas formas de la verdad. Sin embargo, para que eso se convierta en algo útil para la sociedad, se necesita algo más: querer descubrir lo oculto.

Revelar lo que otros esconden es siempre un acto político. Este libro intentó hacer eso con internet y la tecnología. Pero esa es una parte del camino. El resto es defender a la Red, seguir conociendo quiénes son y serán parte de sus guerras. Para eso hay que hacer lo mismo de siempre. Se trata de salir a la calle o —si preferimos— quedarnos en nuestra computadora o en el celular, pero con otra actitud: ser curiosos, ser críticos. Ser menos religiosos y abrazar el escepticismo como un arma —tal vez como una droga— que nos mantenga siempre despiertos.

Agradecimientos

A Federico Kukso, por ese primer chat que nos dio la idea, por su generosidad de colega y por editar mi libro con una inteligencia que me inspiró cada vez a mejorar.

A Juan Boido y Glenda Vieites, por entusiasmarse con el proyecto y apoyarlo con optimismo y las preguntas correctas para hacer también un buen producto.

A Ana Laura Caruso, una editora y amiga detallista y presente, que quiso mi libro desde el primer minuto y lo cuidó en su camino hasta convertirse en realidad.

A Nacho Román, un colega y amigo que iluminó mi libro en cada charla, con su conocimiento, su fe en mi trabajo, su imaginación y su optimismo.

A Natalí Schejtman, Javier Sinay y Matías Chamorro, enormes amigos y colegas que leyeron, ayudaron, me guiaron y estuvieron en momentos buenos y malos. Gracias por las lecturas precisas, el humor y la compañía.

A Nicolás Cassese, mi editor en *Brando* y amigo, que siempre me insistió en que lo más importante era salir a la calle y escribir. Y que para escribir bien —como dice Fabián Casas— había que salir de la comodidad. A mis otros editores con quienes elegí trabajar estos años, por pedirme escribir sobre cosas interesantes y por dejarme proponerles «mis temas»: Fernanda Nicolini, José Natanson y Sebastián Lacunza.

A mis amigas: Natalia Laube, Lourdes Lávaque, Laura Escobar, Violeta Gorodischer, Paula Salischiker y Juliana Fortunato. Escribir es una tarea muy solitaria, y tener amigas que lo entiendan, que compartan las charlas monotemáticas con mates, viajes en auto o salidas al teatro es hermoso y la comprobación de que la amistad es una de las formas más reconfortantes del amor.

A Clara-SchorLandman, mi analista, por insistir con tanta inteligencia y tanto cariño en que lo importante es seguir los deseos hasta conseguirlos.

A mis otros «ayudantes de la vida»: Luis Herbst, Ricky Adler, Mónica Aparicio, Mary Aragón, Mirta Molina, Gonzalo Mallo, Nélida Mamana. Gracias por la salud y por la energía.

A Elisabeth Bohlmann, Fede Lizarralde, Juanma Bertolotti, Diego Prusky, Alejandra Silvera, mis colegas y compañeros de InPulse, que entendieron siempre mi vocación de escribir.

Gracias a quienes fueron colaborando en el trayecto del libro, ofreciendo ayuda, dándome entrevistas, acercándome materiales, compartiendo contactos y charlas: Pablo Martín Fernández, Carolina Martínez Elebi, Félix Ramallo, Bruno Massare, Sebastián de Toma, Ana Clara Pérez Cotten, Agustín Álvarez Rey, Sergio Mohadeb, Valeria Gantman, Virginia Mileto, Violeta Rosenberg, Julia Rosenberg, María Rosenfeldt, Ana Montes, Alejo Tarrío, Julián Paredes, Leandro Africano, Federico

Mayol, Diego Galeano, Juan Butvilofsky, Josefina Giglio, Fernando Peirone, Claudio Veloso, Iara Freiberg, Cristina Nitka.

A Ernesto Curci, Raúl de Pedro, Marcelo Peresutti y todo el equipo Level 3. A Mazalán Comunicaciones, Gonzalo Herrera Morell y Guadalupe Muñoz. A Aida Uzair, Fabiana Sas, Bettina Faure, Antonia Castellanos, y los departamentos de prensa de Telecom y Telefónica de Argentina. A José María Vázquez de Dynamic Marine. A Hernán Seoane, Ariel Graizer, Martín Manuel Rodríguez, Andrés Pugawko, Hernán Moguilevsky y todo el equipo de Cabase. A Hernán Arcidiácono, Pablo Aguirre Paz, Grabriel Vivas, Leandro Fariña y a toda la gente de Iplan. A Diego Martín de Furukawa. A Emmanuel Jaffrot. Al equipo de Arsat. A Norberto Berner y al equipo de prensa de la Secretaría de Comunicaciones. Al Comité Gestor de Internet de Brasil. A Carolina Aguerre; a Alexandra Dans y Rodrigo de la Parra de ICANN; a Sebastián Bellagamba de Internet Society; a Andrés Piazza y Raúl Echeverría de Lacnic. A Beatriz Busaniche y Enrique Chaparro de la Fundación Vía Libre; a Eleonora Rabinovich; a Javier Pallero de Access Now; a Katitza Rodríguez de la Electronic Frontier Foundation; a Katarzyna Szymielewicz de la Fundación Panoptykon; a Claudio Ruiz de Derechos Digitales; a Verónica Xhardez, Laura Marotias, Martín Lima y la gente de SoLAr Argentina; a Guillermo Movía de la Fundación Mozilla; a Andrés Pérez Esquivel; a Eduardo Pedutto, María Julia Giorgelli y Agustina Callegari de la Dirección de Protección de Datos de la Defensoría del Pueblo de la Ciudad de Buenos Aires. A Martín Becerra, Ricardo Beltrán y el equipo de la cátedra de Datos de la UBA; a Gustavo Fontanals; al equipo del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Universidad de Palermo; a Iván Arce y la Fundación Sadosky; a Darío Sztajnszrajber. A Santiago García Vázquez, Walter Cipolla, María Eugenia Ferrari, y todo el equipo del Municipio de Tigre. Al Comisionado Serra, Eduardo Allen, Carolina Sarquis y equipo de prensa de la Policía Metropolitana. A Florencia Bianco y Google Argentina.

A todos los que me mandaron links, notas, me desearon suerte, me preguntaron por el libro y completaron la encuesta que hice cuando empecé a escribirlo.

A mi hermana Jimena Zuazo, por el cariño, por retos, por la compañía.

A Hugo Sánchez, por prestarme su escritorio rodeado de Lamborghini, Fogwill y poesía, las miles de horas que me llevó escribir. Por su afecto construido en cada sobremesa de Tolosa.

A mi abuela, Inés Otellado, que se fue en el capítulo 2, pero se quedó en mi obstinación y en mi fe de que hacer las cosas bien siempre es con amor y con entrega. A mi bisabuelo Eugenio Otellado, por esos diarios de navegación que escribió y encontré cuando empecé a escribir este libro y fueron una señal de que la realidad, si tiene una linda historia, puede ser conmovedora.

A mi mamá, Mirta Castedo, por la pasión y por la mirada política de la vida, que heredé e intento hacer mía. Gracias por la sabiduría, por el amor, por la

incondicionalidad, por la inteligencia, por el compromiso con quienes lo necesitan, por ser el ejemplo real de que transformar el mundo es posible. Le debo a ella una certeza: todos somos capaces de lograr todo; solo necesitamos tener la oportunidad, ser consecuentes y construir las oportunidades para otros.

A Juan, por tanto amor. Y por el futuro.

Condiciones de producción

Este libro fue escrito en una notebook Sony VCPY210FL comprada en 2009, a la que se le rompió el botón de encendido en el capítulo 5. Fue reemplazada por una Samsung Series 5 Ultra, con la que se escribió hasta el final. Por momentos, se trabajó con Windows y Word. En otros, se utilizó Ubuntu y Libre Office.

Las primeras entrevistas se grabaron con un grabador digital Cenix VR-W600E, que se rompió en el capítulo 2 y fue reemplazado por un Daza chino que falló 3 o 4 veces, y a partir de entonces las notas se registraron con la app ASR Recorder en una tableta Nexus 7 de Asus, que también funcionó como cámara de fotos durante todas las notas del libro. En la tableta también se leyeron, comprados en Amazon o bajados gratis, la mayor parte de los libros que se citan en estas páginas. Las películas que menciono fueron todas descargadas de KickAss *torrents* o de PopCorn Time.

Para conectarme a internet, casi siempre utilicé, en la ciudad de Buenos Aires, mi conexión de 10 MB de Speedy. Se desconectó poco, funcionó bien. Algunos fines de semana, en Tolosa (La Plata) usé mucho Cablevisión-Fibertel, de 6 MB, que se cortó permanentemente, haciéndome un favor para no procrastinar pero complicándome la búsqueda de datos. También utilicé la conexión del Sheraton de San Pablo, el Dazzler de Montevideo, varios Starbucks con miles de publicidades invasivas, y muchísimas horas de *wifi* de La Continental.

Para llamar a los entrevistados, usé un teléfono fijo Siemens con una línea de Telefónica, y un Samsung Core con Android con Movistar. Esta última fue la peor conexión de todo el proceso: el 3G debe haber funcionado el 20 % del tiempo. El resto fue esperanza y magia.

Para escribir las ideas que se me fueron ocurriendo, usé mucho los *mails* del teléfono (en donde escribí párrafos enteros) y tres libretas: una roja grande y dos fucsias chiquitas. Cuando terminó el libro, había juntado 13 biblioratos repletos de notas impresas, leyes, artículos, borradores de capítulos. Y comprado unos 40 libros nuevos, que se sumaron a mi biblioteca. La carpeta «LIBRO» de mi computadora (backupeada en un disco externo Verbatim todos los lunes a las 3 pm) ocupaba 16,3 gigas.

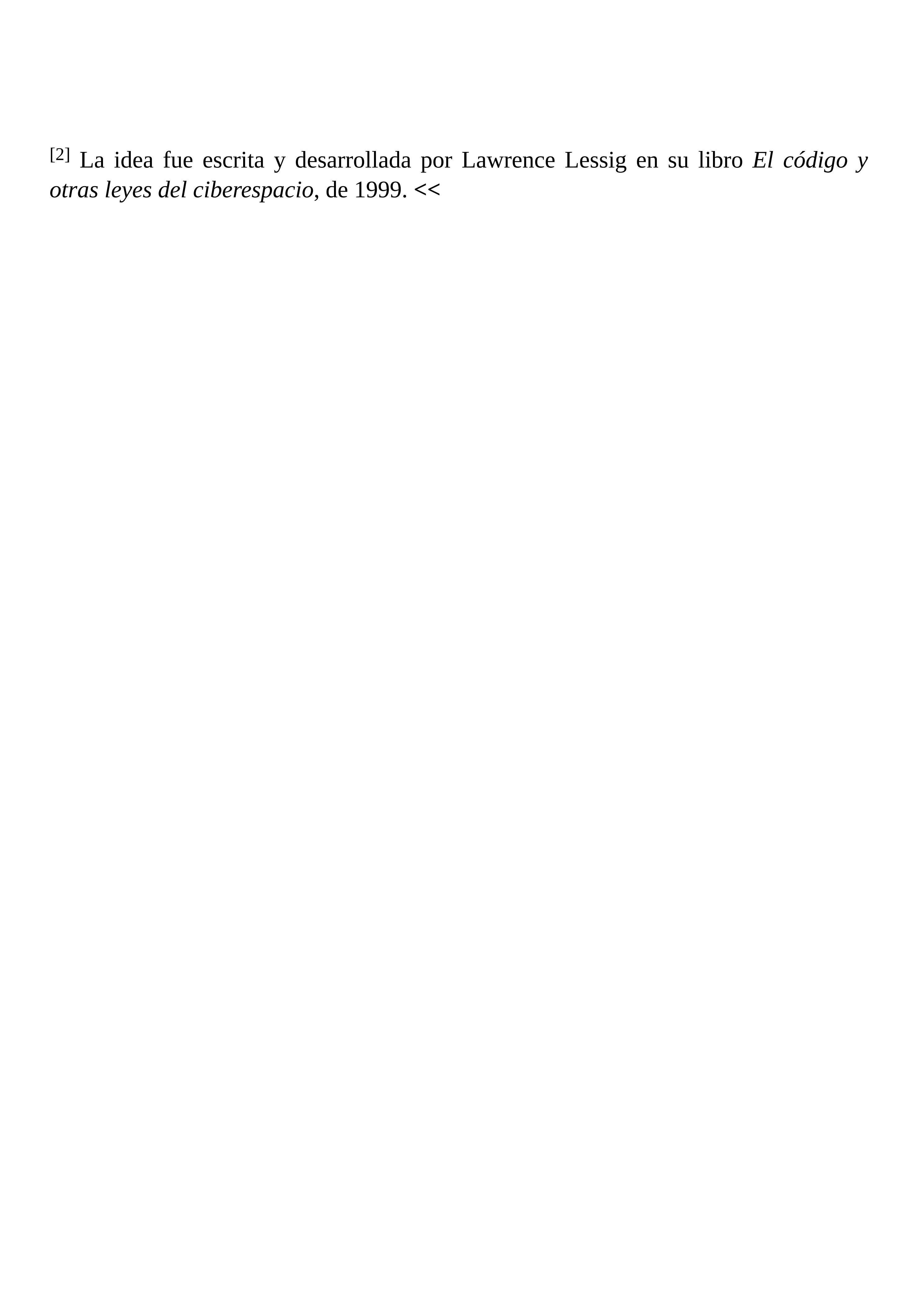


Natalia Zuazo Nació en Tolosa, La Plata, en 1979. Se recibió de licenciada en Ciencia Política con especialización en Relaciones Internacionales en la Universidad de Buenos Aires y realizó el Máster en Periodismo del diario La Nación y la Universidad Torcuato Di Tella. Trabaja en periodismo, estrategia y contenidos digitales desde hace más de diez años. Fue editora de noticias online en Ciudad.com, Clarín.com, Crítica de la Argentina y Perfil.com, y coordinó los proyectos digitales de la revista Anfibia (Unsam/FNPI) y de la Fundación Proa. Es directora de Comunicaciones de una agencia digital. Escribe sobre política, tecnología —y el cruce de ambas— en Le Monde Diplomatique Cono Sur y en la revista Brando, y colaboró en la revista Ñ, y en los diarios La Nación y Ámbito Financiero, entre otros. Condujo Ágora 2.0 en Canal Encuentro, y dio clases sobre medios y tecnología en la Universidad de Buenos Aires y en la Universidad Nacional de La Plata.

Guerras de Internet es su primer libro.

Notas

[1] Escribiremos en cambio «Red», como sinónimo de internet, con mayúscula, para representar a una serie de redes interconectadas, diferenciándola de una red individual. <<



[2] La idea fue escrita y desarrollada por Lawrence Lessig en su libro *El código y otras leyes del ciberespacio*, de 1999. <<

[3] Un algoritmo es un conjunto de reglas que permiten realizar una actividad, como por ejemplo, la búsqueda de un término en Google. Aunque son fórmulas matemáticas, están creadas por hombres para alcanzar un fin, por lo tanto, no implican solo fórmulas, sino también ideologías. <<

[4] Level 3 es un proveedor «mayorista» de infraestructura de internet, del nivel Tier 1, es decir, con capacidad de proveer a otros operadores. Por eso, su nombre no nos resulta tan familiar como el de las otras empresas. <<

[5] Paraguay, por su ubicación mediterránea y sin acceso al mar, no fue parte del cable submarino, algo que explica en gran parte su retraso en el acceso a internet: tiene un 23 % de penetración, contra 68 % de Argentina, 56 % Uruguay y 45 % de Brasil. <<

[6] El resto son: AOL, AT&T, Verizon Business, NTT Communications, Qwest, Cogent, Sprint, Deutsche Telekom, TeliaSonera y Telefónica Global Solutions. <<

[7] Con el cable de vuelta en casa, medí los pelitos de fibra: en un milímetro entraron cuatro. <<

[8] Propiedad de Antel (Uruguay) y Telefónica (Argentina). <<

[9] Popularizada a mediados de los 70 por el director de la Oficina de Presupuesto del presidente norteamericano Jimmy Carter, fue tomada por economistas conservadores y empresas de tecnología para inculcar la idea de que para sobrevivir en el capitalismo basta con hacer algunos pequeños cambios que cada tanto parezcan novedades o innovaciones, pero en el fondo no tocar la esencia del sistema. El concepto está en la base de la estrategia comercial de empresas como Microsoft, que lanzan actualizaciones de sus sistemas operativos con pequeños cambios y las presentan como novedades que todos tenemos que adoptar, o cualquier empresa de celulares ante las nuevas versiones de dispositivos. Pero también sustenta a una estructura como internet, que se creó caóticamente, uniendo una red con otra, hasta transformarse en el gran monstruo actual. Internet tiene, en su ADN, la capacidad de soportar pequeñas fracturas, está diseñada para ser resistente y seguir funcionando. <<

[10] Encuesta Nacional de Consumos Culturales. Secretaría de Cultura de la Nación, 2014. <<

[11] «Concentrated broadband internet market leads to poor service», por Fermín Koop, *Buenos Aires Herald*, 19 de marzo de 2014.Y datos suministrados por las empresas. <<

[12] Indec, 18 de marzo de 2014. La ciudad argentina con la banda ancha más rápida es Cañada de Gómez, en Santa Fe, con 14,43 Mbps. Acassuso, en la zona norte de la provincia de Buenos Aires, se ubica en el segundo lugar, con 10,47, valores similares a las cercanas Beccar, Villa Adelina, Florida, Olivos y Don Torcuato. <<

[13] Fuentes: netindex.com y «Cisco Visual Networking Index: Internet Traffic Growth Forecast, Latin America Forest Update, 2013-2018». <<

[14] Los precios de la conectividad en América Latina y el Caribe. Reporte 2013. Hernán Galperín. Udesa. <<

[15] Cuando fue vendida a Telmex (América Móvil), del magnate mexicano Carlos Slim. <<

[16] Williams, Raymond (ed.) (1992), *Historia de la comunicación*, Editorial Bosch, Barcelona. Capítulo «Tecnologías de la información e instituciones sociales», pp. 182-210. <<

[17] «¿Qué nos ha traído Dios?», fueron las primeras palabras que Morse transmitió por una línea telegráfica, invitando al futuro a hacer el resto. <<

[18] Las centrales de la ciudad de Buenos Aires estaban en la avenida Rivadavia y Libertad, y en San Martín y avenida Córdoba desde 1923. A ellas le siguieron otras centrales ubicadas en los barrios que se iban poblando, bautizadas con sus nombres o los de las calles donde funcionaban: Juncal, Avenida, Palermo, etc. <<

[19] El edificio es la actual sede de la Fundación Telefónica, dedicada a muestras de arte y tecnología de vanguardias. <<

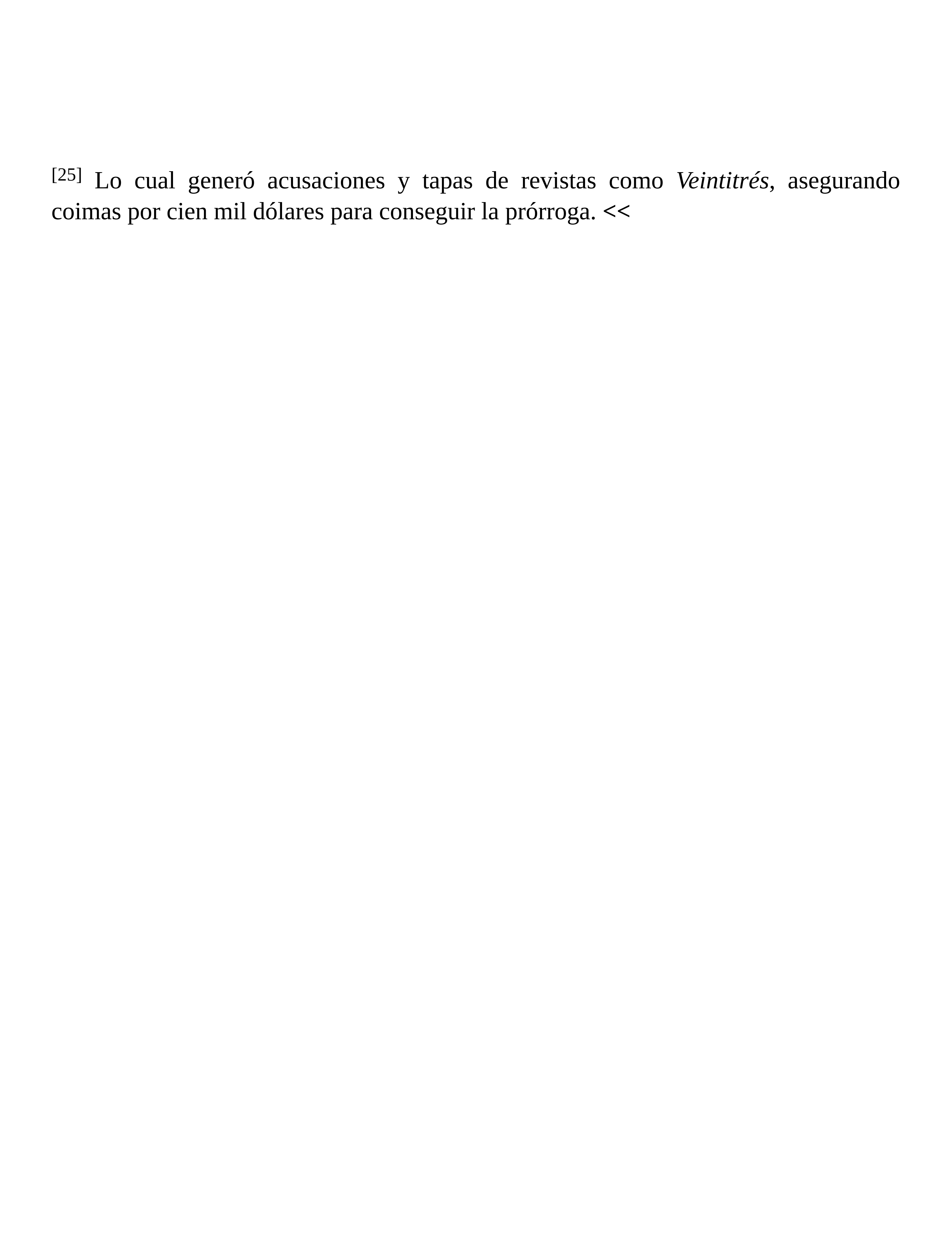
[20] Para una historia de la privatización de Entel y su acompañamiento mediático, ver: «Los medios y la privatización de Entel. El tratamiento noticioso del servicio telefónico argentino antes y después de su transferencia», tesis doctoral de Natalia Aruguete, Universidad Nacional de Quilmes. Disponible en http://bit.ly/1vItpNP. <<

[21] Fueron quienes conservaron su trabajo luego de los despidos masivos que se produjeron con la privatización de Entel, que dejó sin trabajo al 75 por ciento de sus empleados. <<

[22] El proyecto fue impulsado por el entonces canciller Dante Caputo, a quien el grupo le reconoce la visión y la decisión política de impulsar al país a integrarse a las nuevas tecnologías. Caputo quería incorporar computadoras y mejorar las comunicaciones que se hacían a través del Télex y el correo tradicional. <<

[23] Para una historia detallada de internet en la Argentina está la excelente nota de Federico Novick «Un cuartito con vista al mundo», publicada en «Radar» de *Página/12*, el 14 de mayo de 2014. También visitar el programa de historia de la Facultad de Ciencias Exactas de la UBA en exactas.uba.ar y el sitio del Proyecto SAMCA en proyectosamca.com.ar. El periodista de tecnología de *La Nación*, Ariel Torres, también realizó, durante 2014 —con motivo del cumpleaños 25 años de la Red—, una serie de notas sobre la historia de la internet local, que pueden encontrarse en http://www.lanacion.com.ar/autor/ariel-torres-69. <<

[24] En esos años, precisamente en 1989, comenzó la prestación de servicios de comunicaciones móviles en Argentina. La empresa Movicom (Bell South) obtuvo la licencia para prestar el servicio de radiocomunicaciones móviles en la ciudad de Buenos Aires, el Conurbano y la Plata. En 1993, se sumó la empresa Miniphone (perteneciente a Telecom y Telefónica) que obtuvo licencia para prestar el servicio solamente en el AMBA. En el interior del país, dividido en regiones norte y sur, los servicios móviles fueron brindados por la empresa CTI (Compañía de Teléfonos del Interior) desde 1995. A partir de 1996, las empresas Telecom y Telefónica obtuvieron licencias para prestar servicio de telefonía móvil en las zonas geográficas donde brindaban el servicio básico telefónico (telefonía fija), compitiendo con CTI. <<



[25] Lo cual generó acusaciones y tapas de revistas como *Veintitrés*, asegurando coimas por cien mil dólares para conseguir la prórroga. <<

[26] Entre las dos redes, les sobrarían kilómetros como para dar una vuelta al mundo. <<

[27] A cargo del Ministerio de Planificación de la Nación, con participación de la empresa estatal Arsat (Empresa Argentina de Soluciones Satelitales). <<

[28] Como le gusta decir al especialista en seguridad de sistemas Enrique Chaparro, de la Fundación Vía Libre. <<

[29] Del inglés *Internet Service Providers*. <<

[30] Usamos «autopista» como sinónimo estricto de «ruta». Sin embargo, en este libro evitamos utilizar el concepto «autopista de la información», que se suele emplear como sinónimo de internet, ya que no es un término neutral. Popularizado entre 1992 y 1994 por Al Gore, el entonces vicepresidente de la administración Bill Clinton, la idea de «supercarretera» suponía una gran infraestructura que había que ayudar a desarrollar desde el gobierno para que a su vez ayudara al progreso de los ciudadanos, en una asociación lineal: a más infraestructura, más conexiones, más comunicación, más libertad, más crecimiento económico. <<

[31] El mapa actualizado diariamente se encuentra en as-rank.caida.org. <<

[32] Mariano Zukerfeld desarrolla esta idea en «De niveles, regulaciones capitalistas y cables submarinos: Una introducción a la arquitectura política de internet», revista *Virtualis*, junio de 2010. <<

[33] Algunos nostálgicos (y conservadores) de la primera generación de empresarios de internet critican a las nuevas generaciones de «nerds» por su falta de maldad, reflejado en «*Don't be evil*» («No seas malvado»), el eslogan corporativo de Sergey Brin para Google. «Ese es el peor problema con los nerds: no les divierte el odio. Sus clientes en Silicon Valley son emprendedores tecnológicos, tipos famosos por sus Clubes de Matemática de la secundaria pero ignorantes de cómo funciona el poder político», dice el político y periodista estadounidense P. J. O'Rourke, editor de internacionales de la *Rolling Stone* local. <<

[34] La Corporación RAND (Research And Development) es un laboratorio de ideas (*think tank*) norteamericano que forma a las fuerzas armadas norteamericanas. <<

[35] El directorio de Verisign es uno de los lugares elegidos por los exdirectores de la NSA para jubilarse. En 2010 se trasladó a Virginia, donde también se encuentra el Pentágono. La empresa opera una gran variedad de infraestructuras de red vitales, como dos de los trece servidores de nombre raíz de internet y el registro de los dominios de nivel superior .com, .net y .name, entre otros. <<

[36] Del inglés *Network Operations Center*. <<

[37] Iplan tiene 4 *datacenters* en la Ciudad de Buenos Aires, Córdoba y Rosario. El de Fibertel funciona en Barracas, en la sede de Cablevisión, en un edificio que antes había sido del diario *La Razón*. Telefónica tiene tres *datacenters* en Argentina, en Barracas, Villa General Mitre y San Nicolás, todos en la Ciudad de Buenos Aires. Telecom tiene un gran centro de datos en Pacheco —partido de Tigre, Buenos Aires —, en Coghlan —Ciudad de Buenos Aires— y en Bosque Alegre, provincia de Córdoba. Claro tiene un centro de datos en Colegiales y otro en la avenida Paseo Colón, al sur de la Ciudad de Buenos Aires. Cabase, la cámara que agrupa pequeños y medianos proveedores de internet, tiene su *datacenter* en pleno microcentro porteño y una serie de siete NOC distribuidos federalmente en el país. <<



[38] Datos de 2013 de Pingdom, empresa sueca dedicada al monitoreo de datos en internet. <<

[39] Su nombre proviene de la expresión de la teoría de la relatividad de Albert Einstein para representar la equivalencia entre masa y energía. <<

[40] Greenpeace International, «How Dirty is Your Data», 21 de abril de 2011, en: http://bit.ly/1ALTdtO. <<

[41] Democratiza también en tanto el acceso también sea democrático geográficamente, los precios sean similares para conexiones equivalentes, y quienes usen internet tengan un dominio homogéneo de las herramientas y plataformas para acceder a «las conversaciones». <<

[42] «Peleando por la neutralidad», *El País*, 6 de diciembre de 2014: http://www.elpais.com.uy/que-pasa/peleando-neutralidad.html. <<

[43] Datos de Ericsson, en *Information Technology* N.º 205, octubre de 2014. **<<**

[44] «A Super-Simple Way to Understand the Net Neutrality Debate», The Upshot, *The New York Times*, 10 de noviembre de 2014. **<<**

[45] Actualmente, el 60 % de las conexiones residenciales de internet en Estados Unidos son provistas por compañías de TV por cable, como Comcast y Time Warner. El restante 20 % son conexiones DSL de compañías telefónicas. El otro 20 % son cables de fibra óptica, la mayoría de los cuales pertenecen a Verizon o a AT&T. <<

[46] En América Latina, Chile fue el primer país en tener una ley de neutralidad, y se convirtió en un ejemplo en el mundo. El segundo país que contempló la neutralidad en la región fue Ecuador, en 2012, a través de una regulación de la Conatel, su organismo nacional de telecomunicaciones. Dos años más tarde, en 2014, Brasil fue el tercer país de América Latina en tener una disposición que defiende la neutralidad dentro del Marco Civil de internet. En el mundo, Holanda fue el primer Estado europeo en tener su norma en 2012, y luego siguió, también en 2014, el Parlamento Europeo, con una resolución de neutralidad para todo el continente. <<

[47] Como sucedió, al menos en la letra impresa, con la ley Argentina Digital de diciembre de 2014, que todavía requiere avances en la práctica para ver cómo se define la disputa local. <<

[48] Para una historia detallada de Arpanet, ver: «Paul Baran and the origins of the internet», Rand Corporation (http://www.rand.org/about/history/baran.html) y «Una red de redes», capítulo 2 de *Tubos*, de Andrew Blum, Océano, México, 2012. <<

[49] Por las siglas de la red de computadoras, a la que llamaron Advanced Research Projects Agency Network. <<

[50] Las seis leyes de Melvin Katzenberg pueden consultarse en http://en.wikipedia.org/wiki/Kranzberg's_laws_of_technology. <<

[51] Cerf provenía de la Universidad de California y Kahn del Instituto Tecnológico de Massachussets, y sus investigaciones fueron financiadas por DARPA. **<<**

[52] Del inglés *Request For Comments*. Los protocolos más importantes de internet están definidos por RFC, cada uno con un número. El protocolo IP, por ejemplo, está detallado en el RFC 791, el HTTP —escrito por Tim Berners-Lee y otros— en el RFC 2616. <<

[53] Siglas de *HyperText Markup Language* (lenguaje de marcas de hipertexto). **<<**

[54] Como dice el famoso postulado del abogado estadounidense, profesor de derecho de informática en Harvard y activista de internet, Lawrence Lessig. <<

[55] La idea está explicada por la investigadora y activista de internet argentina Verónica Xhardez en «Internet: Redes Informáticas y jerarquías»: http://bit.ly/1Jz0Xod. <<

[56] Manuel Castells, «El impacto de internet en la sociedad: una perspectiva global», en *19 ensayos fundamentales sobre cómo internet está cambiando nuestras vidas*, BBVA, 2014: http://bit.ly/1g3jIjR. <<

[57] Tim Wu es mundialmente reconocido por concebir el concepto «neutralidad de la Red». <<

[58] «Internet se enfrenta a una polémica privatización», *El País*, 1994: http://bit.ly/1zNGxYc. <<

[59] Para explicaciones detalladas de gobernanza técnica de internet ver Kurbalija, J. y Gelbstein, E. (2005): *Gobernanza de internet. Asuntos, actores y brechas*, Diplo Foundation. También Califano, B. y Baladron, M. (2011): «¿Quién controla internet? Gobernanza, políticas y desafíos para el futuro de la red de redes». *Avatares de la comunicación y la cultura*, N.º 2. Y Cortes, Carlos (2014): *La gobernanza de internet: la trampa de las formas*. CELE, Buenos Aires. <<

[60] El primer sistema, llamado IPv4, permitía asignar más de 4 mil millones de direcciones únicas. Pero como ese número se quedó corto para las necesidades de internet (especialmente con la conexión de miles de millones de celulares, tabletas o aparatos que necesitan una dirección), en 2014 se comenzó a implementar el sistema IPv6, que admite 340 sextillones de direcciones, unos 670 mil billones de direcciones por cada milímetro cuadrado de la superficie terrestre (¡como para que alcance!). <<

[61] No todos son países. Hay varias islas, dependientes de países, como las Islas Vírgenes (de Gran Bretaña, Estados Unidos y Puerto Rico) con el sufijo .vi, la isla Reunion de Francia con .re, las islas Heard y McDonald, deshabitadas y propiedad de Australia en el océano Índico con .hm, una ciudad-estado como el Vaticano con .va, etc. <<

[62] A través de registros locales en cada Estado, como Nic.ar en el caso de Argentina, que durante muchos años dependió de la Cancillería local, y en 2013 pasó a depender de la Secretaría Legal y Técnica de la Presidencia de la Nación. En cada país, el registro regional puede depender de distintos organismos. En Brasil, por ejemplo, Nic.br depende de un organismo estatal encargado de todo lo referente a internet, el Comité Gestor de Internet (CGI). <<

[63] Ubicados estratégicamente entre la costa este de la estructura administrativo-militar de Estados Unidos (Maryland) y la oeste de Silicon Valley y los organismos de internet (California), están operados por distintas organizaciones y empresas, por ejemplo ICANN, la NASA, el Laboratorio de Investigación del Ejército Norteamericano, la Agencia de Sistemas de Información de Defensa, la Universidad de Maryland, y las empresas Verisign y Cogent Communications. <<

[64] El mapa completo y actualizado de servidores raíz puede consultarse en http://root-servers.org. <<

[65] En el caso de América Latina, eso sucedió en abril de 2014, cuando un funcionario paraguayo llevó ante otros representantes de instituciones de internet regionales la moción de instalar en su país un *root server* para la región. La propuesta fue rechazada, pero reflejó que todavía existe la idea de que emplazando servidores de raíz locales se logra automáticamente una mayor soberanía o control de internet por fuera de Estados Unidos. <<

[66] A las que hay que agregar también el Word Wide Web Consortium (WC3), fundado en 1994 por Tim Berners-Lee. Es un consorcio internacional de empresas, laboratorios tecnológicos e investigadores que produce recomendaciones para la *World Wide Web*. <<

[67] Organizadas por la Unión Internacional de las Comunicaciones (ITU). <<

[68] La otra postura —de China, Rusia e Irán, entre otros— abogaba por una organización más intergubernamental de la Red. <<

[69] Datos de Nielsen y Deep Field citados por The Conectivist: bit.ly/1pK4ghC. **<<**

[70] En China, el país más poblado del mundo, existen otros sitios y servicios que concentran el tráfico de los usuarios: el mensajero QQ; el sitio de compras Taobao, un Amazon local con más de 800 millones de productos en venta; Weibo, una especie de Twitter usado por el 30 % de los chinos; Renren, llamado «la copia china de Facebook»; Todou, un sitio de videos similar a YouTube; y Baidou, el motor de búsqueda más grande. No casualmente, Mark Zuckerberg, el CEO de Facebook, está aprendiendo chino y se lo pudo ver hablando el idioma (que además comparte con su esposa, de esa nacionalidad) en distintos encuentros en el país, al que apunta a llegar para expandir aún más el mercado de su empresa, que actualmente tiene tantas cuentas como usuarios de internet en el mundo: 1320 millones. <<

[71] Un año después, el 17 de diciembre de 2014, el presidente norteamericano Barack Obama anunció el fin del bloqueo a Cuba, impuesto por su país por 53 años, con lo que terminó con el último símbolo de la Guerra Fría por caer. **<<**



[72] Película documental dirigida por Laura Poitras, estrenada en noviembre de 2014: https://citizenfourfilm.com/. <<

[73] Cárcel para presos políticos de Estados Unidos, en el territorio cubano, denunciada por diversos organismos de derechos humanos por sus condiciones inhumanas y actos de tortura. En su campaña a Presidente, el luego presidente Barack Obama había prometido cerrarla, pero todavía no lo hizo. <<

[74] Creada por J. J. Abrams, el cerebro también detrás de *Lost*. **<<**

[75] En 1971, Daniel Ellsberg y Anthony Russo filtraron archivos de la Guerra de Vietnam, donde demostraban que la administración del presidente norteamericano Lyndon Johnson había mentido sobre la extensión y los ataques en ese conflicto. <<

[76] En 1972, una fuente anónima que se hizo llamar Garganta Profunda filtró a los periodistas Bob Woodward y Carl Bernstein, de *The Washington Post*, información que involucraba al entonces presidente Richard Nixon en espionaje al comité nacional de los demócratas. Tras el escándalo, Nixon renunció a la presidencia. <<

[77] El ensayo completo puede leerse en http://cryptome.org/0002/ja-conspiracies.pdf. <<

[78] *La ética hacker (2001)* es un libro-manifiesto escrito por el filósofo finés Pekka Himanen, donde se plantea una ética de trabajo basada en la pasión y la colaboración, y un espíritu abierto, que considere la función social del compartir, en contraste con la idea de que solo en la ganancia material hay un progreso. Es una biblia de hacktivistas, programadores y militantes del *software* libre en todo el mundo. Disponible en: http://eprints.rclis.org/12851/1/pekka.pdf. <<

[79] El 21 de agosto de 2013, luego de un arresto en condiciones inhumamas denunciado por organizaciones de derechos humanos de todo el mundo, Manning fue condenado a 35 años de prisión, tras asumir que había facilitado los documentos a la organización WikiLeaks. Sin embargo, fue absuelto del cargo más grave: ayudar al enemigo. Un día después de su condena, Manning anunció públicamente su deseo de vivir como una mujer y desde entonces adoptó el nombre Chelsea. <<

[80] En su libro *This Machine Kill Secrets*, Dutton-Penguin, 2012. <<

[81] «Assange, un espía para el pueblo», artículo publicado en *The Guardian* el 19 de junio de 2014 y traducido al español por derechoaleer.org: http://derechoaleer.org/blog/2014/06/assange-dos-anos-en-el-limbo.html. <<



[82] Declaraciones de Julian Assange a Santiago O'Donnell en el diario *Página/12*, el 8 de septiembre de 2014. <<

[83] El *caso Snowden. Así espía Estados Unidos al mundo*. Antoine Lefébure. Capital Intelectual, Buenos Aires, agosto de 2014. <<

[84] «NSA collecting phone records of millions of Verizon customers daily». *The Guardian*: http://bit.ly/1K08U9n. <<

[85] «U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program», *The Washington Post*: http://wapo.st/1F0BDGt. **<<**

[86] El video se puede ver en: http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video. <<

[87] Glenn Greenwald. *Snowden. Sin un lugar donde esconderse*. Ediciones B, Buenos Aires, mayo de 2014. <<

[88] «The most wanted man in the world». *Wired*, agosto de 2014: http://www.wired.com/2014/08/edward-snowden/. <<

[89] «Edward Snowden: A “Nation” interview». *The Nation*, 28 de octubre de 2014. <<

[90] @ioerror en Twitter. <<

[91] Julian Assange. *Criptopunks*, Editorial Marea, Buenos Aires, 2013, p. 15. <<

[92] Las *trollfaces* (caras de trol) son un fenómeno de la cultura de internet basado en un cómic de una caricatura conocida como «rageface» o «cara de ira». Se difundieron a través de foros como 4chan (donde también se iniciaron las primeras acciones de Anonymous y de otros grupos de *hackers*) y se multiplicaron a través de imágenes compartidas masivamente, conocidas como memes. En internet, un trol es una persona que publica mensajes provocadores, irrelevantes o fuera de tema en una comunidad, redes, sitios o blogs, con el objetivo de provocar a otros usuarios, alterar conversaciones, o simplemente para divertirse o molestar. <<

[93] El movimiento de los ciberpunks se inició en 1992 con un grupo de gente interesada en la criptografía y la preservación de la privacidad. Se relacionaron a través de una lista de correo electrónico, con discusiones sobre la criptografía y sus efectos en la sociedad. Tuvo su mayor actividad hasta 1997. <<

[94] @jerezim en Twitter. <<

[95] Junto con Appelbaum y el alemán Andy Müller-Maguhn, es protagonista de las conversaciones que integran *Criptopunks*, el libro/manifiesto de Julian Assange donde llaman a una lucha criptográfica para defender al mundo de la vigilancia masiva. <<

[96] Fundada en 1990, con sede en San Francisco, la EFF es una de las organizaciones más respetadas y activas en la defensa de los derechos y la libertad de expresión en la era digital. <<

[97] La lista completa se puede consultar en: netmundial.br/list-of-participants. E incluye, para la sociedad civil: asociaciones de usuarios de internet, organizaciones de derechos de internet, colectivos de *software* libre, partidos piratas; para los participantes gubernamentales: organismos regulatorios, diplomáticos, cancillerías, embajadas, funcionarios de organismos de seguridad, policía y ejércitos; para los organismos internacionales: representantes de Naciones Unidas, bloques regionales, organismos dependientes de Naciones Unidas como Unesco, organizaciones de internet; para el sector privado: empresas de tecnología, proveedores de internet, redes sociales y buscadores, representantes de cámaras empresarias de tecnología, *software, hardware*, telecomunicaciones, proveedores de infraestructura, empresas de contenido, empresas de comercio electrónico, etcétera. <<

[98] Ocupó el lugar desde 2008 hasta agosto de 2014. **<<**

[99] «Necesitamos una Carta Magna para internet», Tim Berners-Lee, *El País*, 28 de mayo de 2014. O ver su charla TED: «Tim Berners-Lee: Una Carta Magna para la web». <<

[100] No obstante, cuando le pregunté por esta medida a Hartmut Glaser, el secretario ejecutivo del Comité Gestor de Internet de Brasil, me confirmó que este anuncio fue más bien realizado como declaración de soberanía y luego desestimado en medidas reales, ya que es técnicamente casi imposible de implementar (ver «Glaser: necesitamos una internet menos dependiente de Estados Unidos», *Ámbito Financiero,* 15 de mayo de 2014). <<

[101] Declaración completa en: http://www.lacnic.net/web/anuncios/2013-declaracion-montevideo. <<

[102] Documento completo en netmundial.br/NetMundial-multistakeholder-statement/.
<<

[103] «How Laws Restricting Tech Actually Expose Us to Greater Harm», *Wired*, 26 de diciembre de 2015, http://wrd.cm/18YAEuE. <<

[104] http://www.endofabsence.com/. <<

[105] La primera guerra es por la neutralidad de la Red, que tratamos en el capítulo 3 de este libro. <<

[106] «De niveles, regulaciones capitalistas y cables submarinos: Una introducción a la arquitectura política de internet», artículo de Mariano Zukerfeld en la revista *Virtualis*, junio de 2010. <<

[107] «Lo que pasa con Argentina me tocó vivirlo en carne propia», entrevista de Santiago O’Donnell a Julian Assange en *Página/12*, 7 de septiembre de 2014. <<

[108] Además de la concentración en los caminos físicos de los datos, también existe una centralización entre las empresas a quienes confiamos los contenidos. Como ya señalamos, en el mundo, un tercio de todo lo que hacemos diariamente en internet pasa por cinco grandes compañías. En la Argentina, el panorama es una réplica de la tendencia mundial, con algunos agregados locales: el mayor porcentaje de las visitas cotidianas lo concentran Google, Microsoft, Facebook, Yahoo y los dos grupos de medios de comunicación dominantes: *Clarín* y *La Nación* (le siguen Mercado Libre, Taringa y Wikipedia). Según datos de ComsCore, en su reporte «Futuro Digital Argentina 2014»: http://bit.ly/1vHaf9J. <<

[109] El gasto en defensa de Rusia equivale nada más que al 7 % del de la alianza occidental en la OTAN. <<

[110] Seis meses después de las revelaciones de espionaje masivo realizadas por Snowden, el diario *Folha de São Paulo* informó que la Agencia Brasileña de Inteligencia (Abin) vigiló en Brasilia una serie de salas alquiladas por la embajada de Estados Unidos, además de espiar a diplomáticos de Rusia, Irán e Irak. La Presidencia admitió la operación y defendió su legalidad bajo la figura de «contraespionaje». <<

[111] Según datos de la compañía de seguridad informática McAfee. <<

[112] http://www.icic.gob.ar. <<

[113] «Los intermediarios y los desafíos para la libertad de expresión en internet», Ramiro Álvarez Ugarte y Eleonora Rabinovich http://www.cuestiondederechos.org.ar/pdf/numero4/Articulo-8.pdf. <<

[114] «Internet: la tercera vía», *Bastión Digital*, 4 de noviembre de 2013. http://ar.bastiondigital.com/notas/internet-la-tercera. <<

[115] Con este sistema, las demandas por contenidos de usuarios que violen los derechos de autor pueden ser fácilmente procesadas, quitándolas de circulación ante un pedido sencillo de las corporaciones. <<

[116] La información no se borra sino que deja de ser indexada, es decir, reduce su posibilidad de ser tomada en cuenta en futuras búsquedas. Por eso, para algunos especialistas, es más adecuado referirse al «derecho al olvido» como un «derecho a la desindexación». <<

[117] Según datos de la Cepal (Comisión Económica para América Latina y el Caribe). <<

[118] «Derechos humanos en línea: una agenda aún pendiente para la sociedad civil de América Latina y el Caribe», por Valeria Betancourt: http://bit.ly/1Lc4dqB. <<

[119] Ejemplo citado en Álvarez Ugarte y Rabinovich, *op. cit*. <<

[120] Cámara Argentina de Productores de Fonogramas (Capif), la Sociedad Argentina de Autores y Compositores de Música (Sadaic) y seis discográficas (Warner, EMI, Universal, Leader Music, Sony, Epsa). <<

[121] Y publicaron el sitio de denuncia chupalacapif.com. **<<**

[122] Para un informe completo, ver Freedom of the Net 2014, de Freedom House http://bit.ly/1rGAp00. <<

[123] Parker, nacido en 1979, después fue uno de los fundadores de Facebook y actualmente es uno de los accionistas del servicio de música por *streaming* Spotify. <<

[124] Para una historia de Napster, ver el documental *Downloaded* (2013), dirigido por Alex Winter. <<

[125] Manovich, Lev. *El lenguaje de los nuevos medios de comunicación*, Barcelona, Paidós, 2006. <<

[126] Baricco, Alessandro. *Los bárbaros*, Barcelona, Anagrama, 2008. <<

[127] Uno de los casos más resonantes fue el del megajuicio que inició Viacom (compañía dueña de canales como MTV) contra YouTube/Google en 2007, por el que reclamaba mil millones de dólares en concepto de daños por «violación masiva internacional de *copyright*». En 2013 la justicia de Estados Unidos falló a favor del sitio de videos, alegando que, en su condición de intermediario, no era responsable de los contenidos (protegidos o no por *copyright*) que subieran sus usuarios. <<

[128] Junto con la medicina y la salud (industria de los medicamentos, vacunas, avances médicos), y la alimentación (soja, transgénicos, Monsanto), la tecnología y el *software* (Microsoft, Apple). <<

[129] Lars Ulrich, baterista de la banda Metallica, dijo sobre el juicio que siguieron contra el sitio de descargas: «Napster nos jodió, entonces nosotros los jodimos a ellos». <<

[130] En marzo de 2014, el director de cine argentino ganador de un Oscar, Juan José Campanella, atacó a la aplicación de películas Popcorn Time. «Te felicito Sebastián, creador de Popcorn Time. Sos un chorro argentino más en nuestro larga lista», dijo el cineasta desde tu cuenta de Twitter, generando una polémica que finalmente ayudó a publicitar el sitio, que en sus 6 primeros días de vida tuvo 150 mil descargas de la aplicación. <<

[131] El concepto, de Jane Ginsburg (2001), está desarrollado en detalle en el artículo «Libertad de expresión, cultura digital y derechos de autor», de Beatriz Busaniche, en *Cuestión de Derechos* N.º 4, primer semestre de 2013: http://www.cuestiondederechos.org.ar/pdf/numero4/Articulo-3.pdf. <<

[132] Lessig, Lawrence, *Cultura Libre*. Disponible en español en: https://www.derechosdigitales.org/culturalibre/. <<

[133] El académico diferencia cuatro tipos de usuarios que comparten contenidos en la Red: quienes la usan como sustituto de compra de contenidos (cuando sale un disco o una película, lo bajan en vez de comprarlo); los que usan la Red para «probar» la música antes de comprarla (y luego la compran o no); quienes la usan para acceder a materiales con *copyright* que ya no están a la venta o que no habrían comprado porque tienen un precio muy elevado fuera de internet; y los que usan el intercambio *online* para acceder a contenidos que no tienen directamente *copyright*. <<

[134] Doctorow, Cory. «Copyright wars are damaging the health of the internet», *The Guardian*, 28 de marzo de 2013. **<<**

[135] La web como la conocemos —gran espacio universal donde se crean y comparten contenidos minuto a minuto— existe como tal desde hace unos diez años. Los blogs y las redes sociales como Facebook y Twitter tienen menos años de los que imaginamos: los primeros tuvieron su año de gloria en 2008 y las grandes redes sociales tuvieron su momento de gran expansión hacia 2010. <<

[136] «Internet's original sin», publicado en *The Atlantic* el 14 de agosto de 2014: theatln.tc/1sZ4DZW. <<

[137] La «burbuja puntocom» fue un período, entre 1997 y 2001, donde se fundaron, crecieron y alcanzaron grandes niveles de rentabilidad en la bolsa de valores de una serie de compañías de la entonces «nueva» internet. Sin embargo, luego del rápido crecimiento y ganancias, muchas de esas empresas quebraron o cerraron, y, aunque no llegaron a provocar una crisis económica, marcaron un período de recesión en la economía internacional y una etapa de crecimiento más moderado en las empresas de internet. <<

[138] Mikko Hypponen: How the NSA betrayed the world’s trust, charla TED, http://bit.ly/1ChbT9N. <<

[139] Rebecca MacKinnon, *Consent of the Networked*, Basic Books, 2012, p. 13. <<

[140] Rebecca MacKinnon, *op. cit.*, p. 23. <<

[141] ¿Cómo nos vigilan en internet?, Fundación Karisma, http://bit.ly/1Hlu4hH. <<

[142] En: https://es.necessaryandproportionate.org/text. <<

[143] «Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición», se señala en el documento Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. <<

[144] Por ejemplo: no es necesario vigilar a todos los de un grupo o un país ante la posibilidad del delito de una persona. También el documento establece que solo debe realizarse cuando se hayan agotado otras instancias menos intrusivas, y que «cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud», y que «la información será accesada solo por la autoridad específica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización», entre otras cosas. <<

[145] Consultar la ley en http://bit.ly/datosperson. <<

[146] Consultar la ley en http://www.protecciondedatos.com.ar/ley1845.htm. <<

[147] http://www.cpdp.gob.ar/. <<

[148] «Who should own the internet?», Julian Assange, *The New York Times*, 4 de diciembre de 2014. http://nyti.ms/1yUMFe4 <<

[149] *Nothing to hide. The false trade off between privacy and security*, Yale University Press, Estados Unidos, 2011. <<

[150] Tigre, su Delta y sus islas son uno de los destinos turísticos más populares de la provincia de Buenos Aires. <<

[151] Al cierre de este libro, en marzo de 2015, Sergio Massa (Frente Renovador) era el tercer candidato en la lista de precandidatos presidenciales con mayor intención de voto, detrás de Mauricio Macri (PRO) y Daniel Scioli (Frente para la Victoria). <<

[152] Nacido en 1972 en el partido de San Martín, educado en un colegio católico, con una primera militancia en partido liberal conservador Ucedé, fue electo diputado por la provincia de Buenos Aires en 2005 y designado director ejecutivo de la Anses entre 2002 y 2007. Ese mismo año, fue electo por primera vez como intendente de Tigre, tras derrotar al vecinalismo local, debilitado luego de la muerte de su histórico líder, Ricardo Ubieto, el intendente que había gobernado el partido cuatro mandatos consecutivos desde 1987. Entre 2008 y 2009, convocado por el kirchnerismo, asumió como Jefe de Gabinete de la primera presidencia de Cristina Fernández de Kirchner. En 2009 reasumió la intendencia de Tigre, cargo para el que fue reelegido en 2011. En 2013, tras ser elegido nuevamente diputado, asumió el cargo Julio Zamora, integrante de su partido, el Frente Renovador. <<

[153] Datos obtenidos del censo 2010, el sitio periodístico Chequeado.com, y los libros *Massa, el salto del tigre*, de Pablo de León (Buenos Aires, Aguilar, 2013), y *Massa x Massa*, de Juan Cruz Sanz (Buenos Aires, Sudamericana, 2013). **<<**

[154] El término fue acuñado por el periodista Martín Rodríguez en la nota «Tercer tiempo» de *Le Monde Diplomatique*, Edición Cono Sur, N.º 155, de mayo de 2012. <<

[155] El concepto está desarrollado en *El acoso de las fantasías*, de Editorial Akal, y está analizado en sus consecuencias políticas por el periodista José Natanson en la nota «Chocolate laxante», publicada en *Página/12* el 1 de febrero de 2015. **<<**

[156] Hay otros tres centros de monitoreo, más pequeños, en las comunas 4 (Barracas, La Boca, Nueva Pompeya y Parque Patricios), 15 (Agronomía, Chacarita, La Paternal, Parque Chas, Villa Crespo y Villa Ortúzar) y 12 (Coghlan, Saavedra, Villa Urquiza y Villa Pueyrredón). <<

[157] Entre los de la Justicia local, la de la provincia y la contravencional, durante 2014 el Centro de Monitoreo recibió 28 000 pedidos de imágenes de cámaras para acompañar causas judiciales. El número se incrementó a medida que creció el número de cámaras en la ciudad: en 2010 se pidieron 400, en 2011 5700, en 2012 14 000 y en 2013 22 000. <<

[158] «Porteños bajo el foco de las cámaras de vigilancia: cómo funciona el sistema de monitoreo», por Félix Ramallo, *Infotechnoogy*, 29 de agosto de 2013, http://bit.ly/1KBF3ji. <<

[159] Se utilizó, por ejemplo, en el desalojo de 700 familias la villa Papa Francisco, en Villa Lugano, en agosto de 2014, un operativo encabezado por el Gobierno de la ciudad de Buenos Aires, que culminó con incidentes y siete heridos. <<

[160] «El desaparejo uso de las cámaras de monitoreo», por Guillermo Gammacurta, *Ámbito Financiero*, 11 de septiembre de 2013, http://bit.ly/1KuwyZm. **<<**

[161] «Hay que poner camaritas por todos lados», *Mdz Online*, 3 de diciembre de 2012, http://bit.ly/1AbTO9S. <<

[162] La familia de Henry se había refugiado en la Argentina en Nordelta, una ciudad-country ubicada en Tigre donde, en contraposición a lo que sucede en el resto del municipio, no hay cámaras de seguridad y se la señala como uno de los lugares que eligen algunos de los narcos más buscados del mundo. Paradójicamente, la celda del penal de máxima seguridad de Ezeiza donde está preso desde febrero de 2013 es un espacio de tres metros por ocho, sin luz natural y con siete cámaras de vigilancia que lo controlan las 24 horas. <<

[163] http://safecities.economist.com/. <<

[164] Entre las «soluciones para empresas y gobiernos» que vende la compañía tecnológica se destaca una rama importante de su negocio dedicada al «Control de ciudadanos e inmigrantes»: escáneres de huellas digitales y de ADN portables, sistemas de reconocimiento facial, terminales de control biométrico (para organismos de gobierno, aeropuertos, empresas), sistemas biométricos para fronteras y aeropuertos, cámaras de vigilancia y una serie de *softwares* altamente sofisticados para el análisis de datos de cámaras (destinados a detectar y alertar movimientos sospechosos en espacios públicos y privados). <<

[165] «Según Berni, “Buenos Aires es una de las ciudades más seguras de Sudamérica”», *La Nación*, 21 de julio de 2012. <<

[166] Según datos de la Procuración General de la Corte de la Provincia de Buenos Aires, de 2013. <<

[167] De 2014, del brasilero José Padilha, el mismo director de *Tropa de elite*. **<<**

[168] «No, ministers-more surveillance will not make us safer», *The Guardian*, 3 de febrero de 2015, http://bit.ly/1M4sPDv. <<

[169] Motorola, Conectia Wireless y Unitech son otros de los jugadores importantes del mercado de la videovigilancia. <<

[170] Ver «El negocio millonario de la inseguridad», revista *La Tecla*, http://bit.ly/1FQ2i8u. «Videovigilancia: ¿quién se beneficia con el negocio?», por Javier Sinay, *Crimen y Razón*, 27 de marzo de 2014, http://bit.ly/1FQ2u7K. «Radiografía del negocio de las cámaras de seguridad en el conurbano bonaerense», *Mdz Online*, 26 de abril de 2010, http://bit.ly/19lxOAI. <<

[171] Algunos de sus clientes son Avellaneda, Ensenada, Berazategui, Florencio Varela, Almirante Brown, Merlo y Tres de Febrero. <<

[172] «Montoto, el hombre de las dos revoluciones», por Jorge Urien Berri, *La Nación*, 14 de mayo de 2006, http://bit.ly/1MoMb6p. <<

[173] «El exmontonero Mario Montoto pide no demonizar a La Cámpora», por Federico Mayo y Rodis Recalt, revista *Noticias*, 12 de noviembre de 2014, http://bit.ly/1JjfzvY. <<

[174] En las licitaciones para la compra de cámaras, contar con experiencia previa en la provisión de sistemas de CCTV al Estado es un ítem de peso a la hora de volver a ser adjudicada una empresa. Global View, por lo tanto, corre con una ventaja sustancial en este aspecto. <<

[175] «NEC compra la empresa de seguridad de Mario Montoto», IECO, *Clarín*, 9 de febrero de 2012, http://clar.in/1DwGKOy. <<

[176] Montoto ocupa, además, desde 2007, la vicepresidencia lª de la Cámara de Comercio Argentino-Israelí. <<

[177] «Montoto dijo que ganó una licitación de cámaras que todavía no se definió», *La Política Online*, 24 de febrero de 2011, http://bit.ly/1vxKdG8. <<

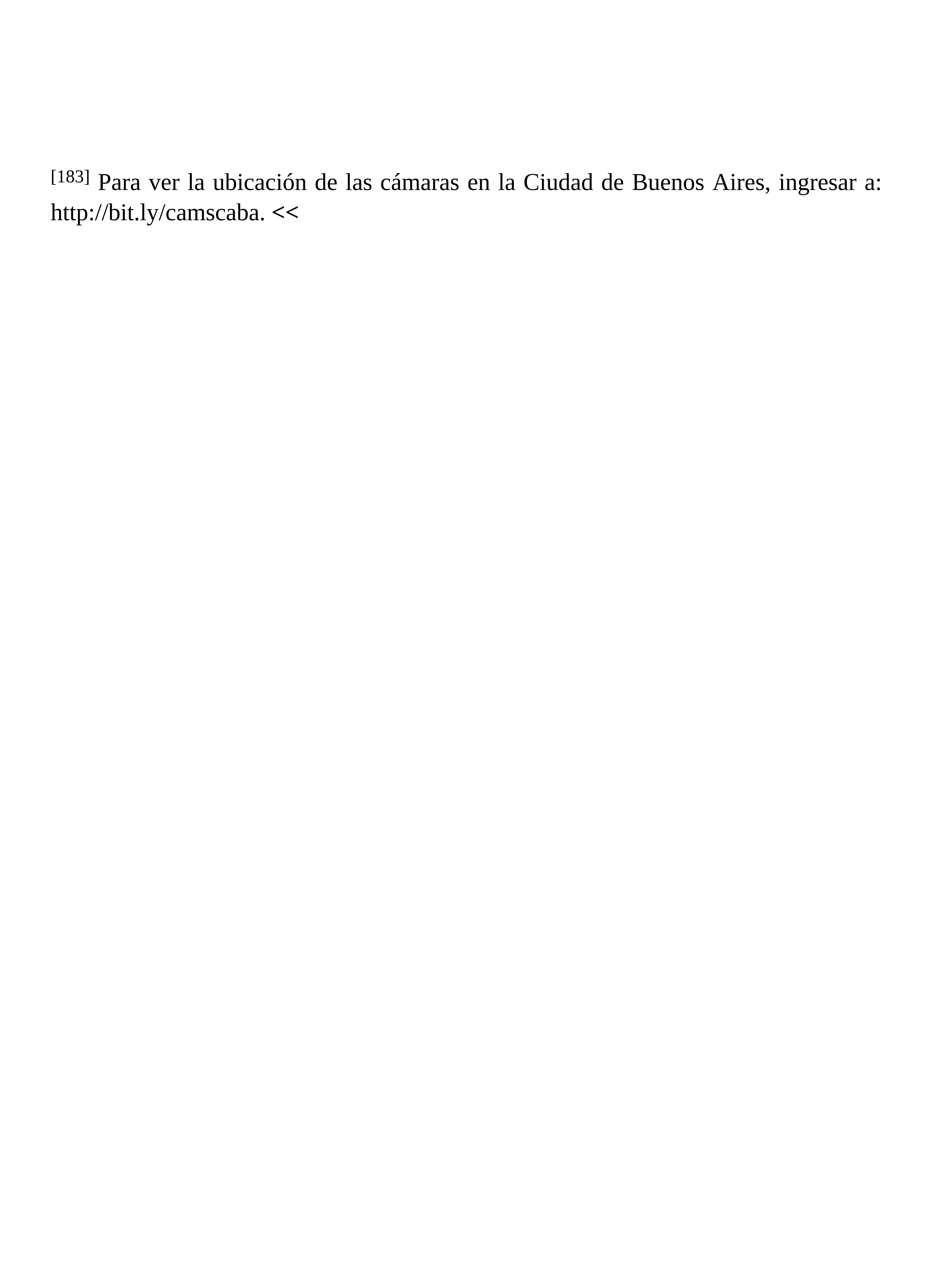
[178] *Smart Cities. Big data, civic hackers, and the new quest for utopia,* Anthony Townsend, W. W. Norton & Company, New York, 2014. **<<**

[179] El aviso, dirigido por el creativo argentino Martín Mercado, también ganó un León de Oro (uno de los premios más importantes de la industria de la publicidad) en Cannes 2012. <<

[180] Otras formas de vigilancia sobre los cuerpos —de las que no nos ocuparemos en este libro por razones de espacio— son los sistemas biométricos aplicados por el Estado nacional en Argentina. Entre ellos, los más importantes son el sistema SIBIOS y las distintas versiones del DNI. El Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS) fue creado por decreto del Poder Ejecutivo Nacional en 2011 con el objeto de «prestar un servicio centralizado de información» de patrones y registros biológicos de los ciudadanos, para identificarlos en la «investigación científica de delitos y el apoyo a la función preventiva de seguridad». Es una base de datos centralizada que almacena, en un único lugar, todos los datos necesarios para identificar a una persona: nombre y apellido, estado civil, grupo sanguíneo, fotografía, huella dactilar y demás recursos relacionados para el reconocimiento digital y automático de cualquier ciudadano argentino. Responde al Ministerio de Seguridad de la Nación y tiene como usuarios primarios a la Policía Federal Argentina, la Gendarmería Nacional, la Prefectura Naval Argentina, el Registro Nacional de las Personas, la Policía de Seguridad Aeroportuaria y la Dirección Nacional de Migraciones. Utiliza distintas vías de recolección de datos: la renovación del DNI y el Pasaporte, que brindan la fotografía de la persona y sus huellas dactilares digitalizadas; las huellas dactilares registradas por la Policía Federal Argentina para su Sistema Automatizado de Identificación de Huellas Digitales (AFIS); el control de ingresos y egresos efectuado por Migraciones con sus dispositivos electrónicos; las imágenes captadas por cámaras de videovigilancia. En palabras de Julian Assange acerca de SIBIOS: «Argentina tiene el régimen de vigilancia más agresivo de América Latina» debido a «las medidas de identificación que se han lanzado en el país, como los sistemas biométricos para los pasaportes». Respecto del DNI, el 27 de junio de 2014, el ministro del Interior y Transporte, Florencio Randazzo, firmó un convenio con la Casa de la Moneda de España para que, a partir de 2015, el nuevo DNI sea «inteligente». Esto implica la inclusión de dos chips: uno donde se encontrarán los datos personales y, en el otro, la información correspondiente a la historia clínica, la ANSES, el PAMI y la tarjeta SUBE. El almacenamiento de esa cantidad de datos personales en una misma base de datos implica también un fuerte poder de parte del Estado al concentrar datos privados en una gran base de datos pública y unificada. <<

[181] Otras provincias que tienen regulaciones para el uso de las cámaras de seguridad son Córdoba, Mendoza, Santa Fe, Corrientes, Tierra del Fuego, Neuquén y San Luis. <<

[182] En materia de videovigilancia también aplica la protección del derecho a la intimidad y no ser molestado de la Constitución de la Nación en su artículo 19. Además, pactos internacionales como la Declaración Universal de los Derechos Humanos, que en su artículo 12 dispone que «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques», y derechos similares reflejados en la Declaración Americana de los Derechos y Deberes del Hombre y en el Pacto Internacional de Derechos Civiles y Políticos. <<



[183] Para ver la ubicación de las cámaras en la Ciudad de Buenos Aires, ingresar a: http://bit.ly/camscaba. <<

[184] «Por qué no podemos saber dónde están las cámaras», por Andrés Pérez Esquivel, diario *Perfil*, 30 de noviembre de 2013, http://bit.ly/1LuxCNg. «La confidencialidad PRO», por A. P. Esquivel, *Página 12*, 30 de junio de 2014, http://bit.ly/1zxzVYj. <<

[185] Creada en 2007 y disponible en 140 ciudades del mundo. <<

[186] En el libro *Historias de cronopios y de famas*. <<

[187] García Canclini, Néstor. *Lectores, espectadores e internautas,* Barcelona, Gedisa, 2007. <<

[188] Según datos de julio de 2014. <<

[189] *Big data* es el área de la tecnología que procesa enormes cantidades de datos que van dejando («voluntariamente», cuando aceptan los términos y condiciones) los usuarios a través de sus «huellas digitales *online*», con el diario uso de dispositivos, herramientas y plataformas digitales. Su utilización más extendida se aplica al *marketing* digital, para predecir deseos y gustos de los consumidores y ofrecerles productos y servicios orientados a su «*target*» o perfil de consumidor. En Europa, el 57 % de los comercios ya utiliza algún sistema para procesar los datos que generan los 369 millones de internautas del continente. La contracara y frontera legal está en el consentimiento del consumidor (que haya aceptado brindar esa información) y en establecer tendencias o patrones —y no identificaciones personales— de un individuo en particular. <<

[190] Magnani, Esteban, Tensión en la red, 2014, disponible en http://www.estebanmagnani.com.ar/. <<

[191] Según datos de *Forbes*, de marzo de 2015, su riqueza supera los 33 mil millones de dólares. <<

[192] Lanier, Jaron. ¿*Quién controla el futuro*?, Buenos Aires, Debate, 2015. <<

[193] Días antes del pico de la gripe aviar en México en 2009, Google ya había registrado el incremento de las búsquedas y podía prever la llegada de la epidemia a ese país. <<

[194] Internet.org es una asociación entre Facebook y seis gigantes de la telefonía móvil. Lanzada en 2013, pretende llevar conectividad a los lugares del mundo todavía sin ella, pero a cambio de que todos los usuarios lo hagan «pasando» por su plataforma, y en cierto modo, por su negocio, con lo que generó grandes críticas desde su lanzamiento. <<

[195] Por supuesto, existen miles de otros en el mundo *online*, tanto o más peligrosos, pero nos centraremos en tres como ejemplos, dada la cantidad de usuarios que utilizan estos servicios en el mundo, y especialmente en Argentina. <<

[196] Vaidhyanathan, Siva. *La googlización de todo (y por qué deberíamos preocuparnos)*, Océano, México, 2010. <<

[197] En el puesto 19 y 20 de los más ricos del mundo, según *Forbes* (marzo de 2015).
<<

[198] 137 mil millones de dólares en 2014. <<

[199] «Google, mighty now, but not forever», *The New York Times*, 11 de febrero de 2015: http://nyti.ms/1FeQaPy. <<

[200] Una *cookie* es una pequeña porción de información que envía un sitio web y queda almacenada en el navegador del usuario para que ese sitio pueda consultar la actividad previa de esa persona-computadora-usuario. Se utiliza para no tener que introducir cada vez los datos de registro, pero al mismo tiempo para controlar a los usuarios, ya que guarda la información de los hábitos de navegación, las páginas visitadas, etc. Las *cookies* son una herramienta vital en el mercado de la publicidad *online*, para conseguir y monitorear los hábitos de los usuarios. <<

[201] Android, Picasa, Panoramio, Stackdriver, Admob, Doubleclick, Nest, Songza, YouTube, entre otras. <<

[202] «Who should own the internet?», *The New York Times*, 4 de diciembre de 2014: http://nyti.ms/1HTlBPa. <<

[203] Capital Intelectual, Buenos Aires, 2014. **<<**

[204] «Los riesgos del tecnofundamentalismo», *Revista Ñ*, 25 de enero de 2013, http://clar.in/1COOT1I. <<

[205] «My map or yours», *Slate*, 28 de mayo de 2013: http://slate.me/1CgySCM. **<<**

[206] Según la política de privacidad que rige desde el lº de enero de 2015. La información puede verse procesada para facilitar su comprensión en la página de la Dirección Nacional de Protección de Datos Personales: www.jus.gob.ar/datospersonales. <<

[207] «Last Week Tonight with John Oliver: Net Neutrality»: http://bit.ly/1GaCjs8. <<

[208] https://disconnect.me/. <<

[209] Según el estudio «The Cost of Reading Privacy Policies», de Aleecia M. McDonald y Lorrie Faith Cranor, http://bit.ly/1Ei7bEL. <<

[210] http://www.thefilterbubble.com/. <<

[211] Según el estudio Cyberspace 2015 de Microsoft Research: http://bit.ly/1xtyWHR. <<

[212] http://datacoup.com/. <<